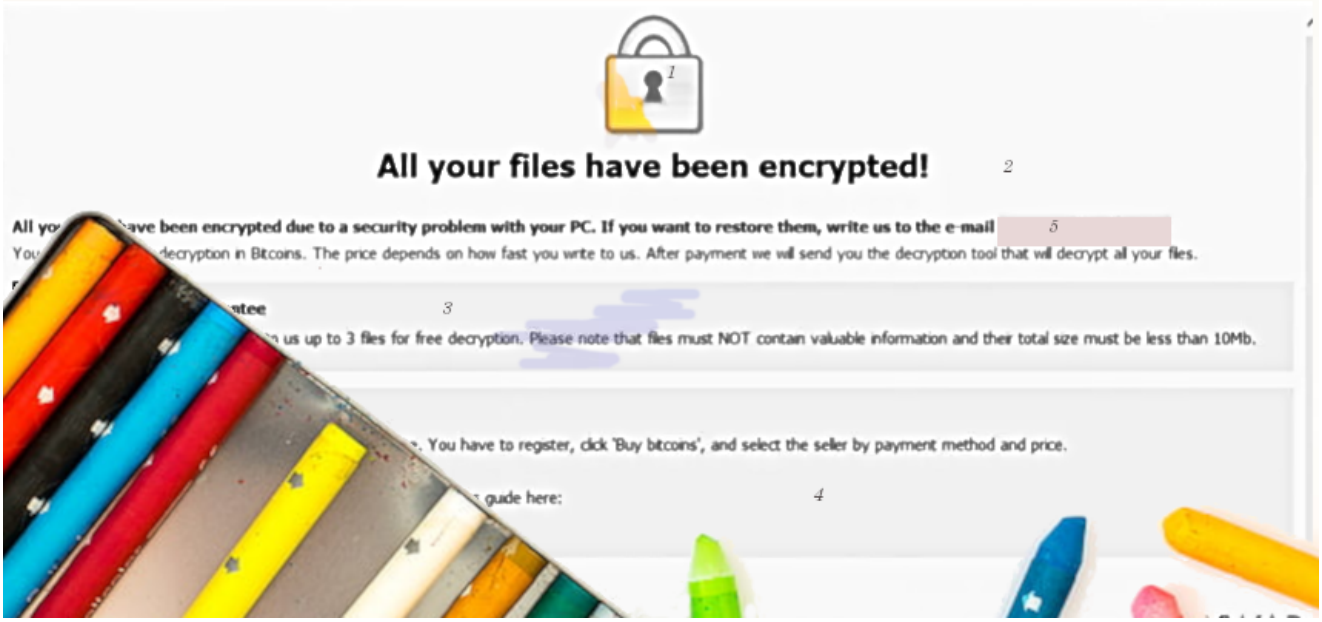
Color by numbers: inside a Dharma ransomware-as-a-service attack

news.sophos.com/en-us/2020/08/12/color-by-numbers-inside-a-dharma-ransomware-as-a-service-attack/

Sean Gallagher August 12, 2020



Dharma, a family of ransomware first spotted in 2016, continues to be a threat to many organizations—especially small and medium-sized businesses. Part of the reason for its longevity is that its variants have become the basis for ransomware-as-a-service (RaaS) operations—the fast-food franchise of cybercrime. Three recent attacks documented by SophosLabs and Sophos MTR have revealed a toolset used by Dharma "affliliates" that explains why attacks from so many different Dharma actors seem so identical, down to the tools and commands they use.

While other, newer ransomware families have grabbed recent headlines with high-profile victims and multi-million-dollar demands, Dharma has continued to be among the most profitable. In part that's because actors with access to the source code continue to innovate around delivering the ransomware as a packaged business for less-sophisticated criminal operators. The Dharma RaaS we've investigated is targeted at entry-level cyber-criminals, and provides a paint-by-the-numbers approach to penetrating victims' networks and launching ransomware attacks.

The actors using this particular RaaS are equipped with a package of pre-built scripts and "grey hat" tools that requires relatively little skill to operate. The Dharma operations we've documented use a combination of internal Windows tools, legitimate third-party "freeware" software, well-known security tools and publicly-available exploits, integrated together through bespoke PowerShell, batch, and AutoIT scripts. This pre-packaged toolkit, combined with back-end technical support, significantly extends the reach of the Dharma RaaS

operators, allowing them to profit while their afililates do the hands-on-keyboard work of breaching networks, dropping ransomware, and managing “customer service” with the victims.

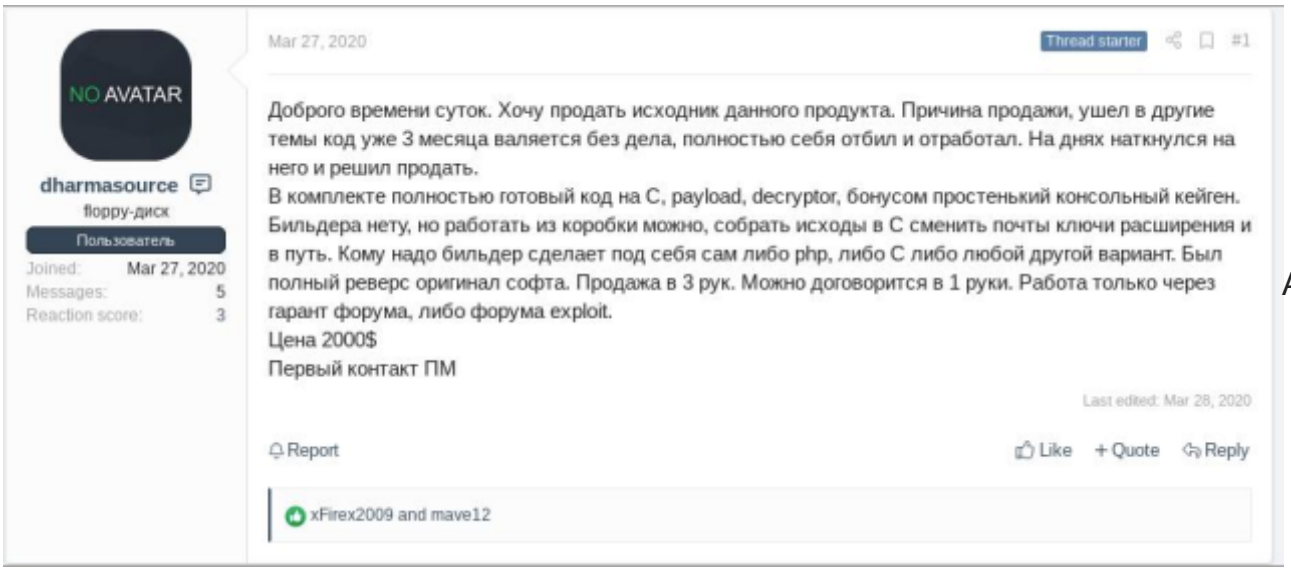
Dharma RaaS Attack Tools Killchain

Initial Access	Execution	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Exfiltration	Impact
RDP credential spraying	PowerShell	CVE-2019-1388	Disables malware protection	Mimikatz	PCHunter	Group Policy Objects	PowerShell screenshot emailer	Dharma Ransomware
Stolen RDP credentials	WMI	CVE-2018-8120	Revo Uninstaller	Remote Desktop Passview	Process Hacker	Remote Desktop	TOR	
	AutoIT	CVE-2017-0213	IOBit Uninstaller	LaZagne	GMER	WinRM Remote Management	dropmefiles [.]com	
	Command line / RDP			NLBrute	Advanced IP Scanner			
				Hash Suite Tools	NS2.EXE			

sophoslabs

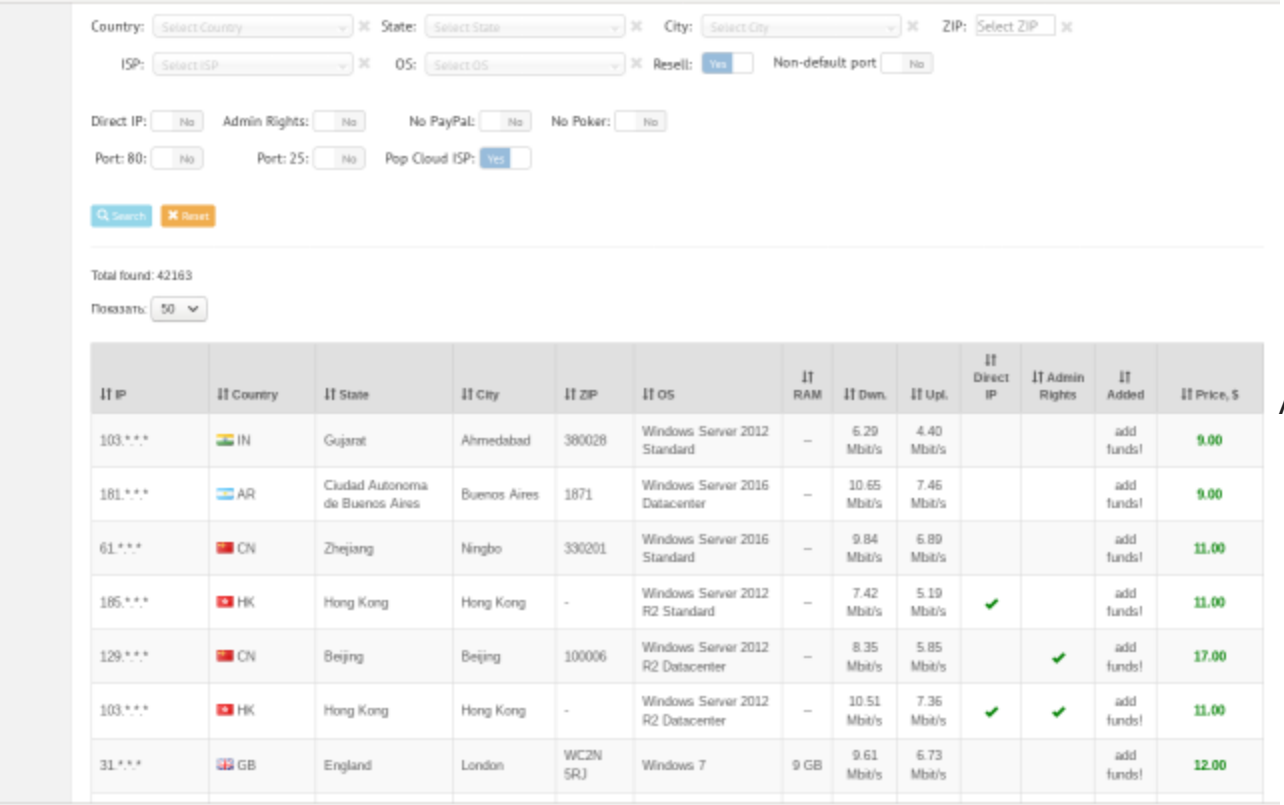
Ransomware economics

Dharma, formerly known as CrySis, has many variants, due to the sale and modification of its source code to multiple malware developers. Those transfers aren’t necessarily from the malware’s original authors, either—in March, a collection of source code for one variant of Dharma was offered for sale on Russian-language crime forums for $2000 through an intermediary.



A forum post from March 2020 offering the Dharma ransomware sourcecode for $2000.

Because of its availability, Dharma has become the center of a criminal ecosystem based on a “syndication” business model. Dharma RaaS providers offer the technical expertise and support, operating the back-end systems that support ransomware attacks. “Affiliates” (often entry-level cybercriminals) pay for the use of the RaaS, and carry out the targeted attacks themselves, using a standard toolkit. Other actors provide stolen credentials and other tools on criminal forums that enable the Remote Desktop Protocol attacks that are the predominant means of initial compromise for Dharma actors. (RDP attacks are the root cause of about 85 percent of Dharma attacks, based on statistics provided by Coveware.)



IP	Country	State	City	ZIP	OS	RAM	Dwn.	Upl.	Direct IP	Admin Rights	Added	Price, $
103.*.*.*	IN	Gujarat	Ahmedabad	380028	Windows Server 2012 Standard	–	6.29 Mbit/s	4.40 Mbit/s			add funds!	9.00
181.*.*.*	AR	Ciudad Autonoma de Buenos Aires	Buenos Aires	1871	Windows Server 2016 Datacenter	–	10.65 Mbit/s	7.46 Mbit/s			add funds!	9.00
61.*.*.*	CN	Zhejiang	Ningbo	330201	Windows Server 2016 Standard	–	9.84 Mbit/s	6.89 Mbit/s			add funds!	11.00
185.*.*.*	HK	Hong Kong	Hong Kong	-	Windows Server 2012 R2 Standard	–	7.42 Mbit/s	5.19 Mbit/s	✔		add funds!	11.00
129.*.*.*	CN	Beijing	Beijing	100006	Windows Server 2012 R2 Datacenter	–	8.35 Mbit/s	5.85 Mbit/s		✔	add funds!	17.00
103.*.*.*	HK	Hong Kong	Hong Kong	-	Windows Server 2012 R2 Datacenter	–	10.51 Mbit/s	7.36 Mbit/s	✔	✔	add funds!	11.00
31.*.*.*	GB	England	London	WC2N 5RJ	Windows 7	9 GB	9.61 Mbit/s	6.73 Mbit/s			add funds!	12.00

A dark web site selling RDP credentials, including some with administrative privileges. These marketplaces in some cases allow buyers to verify the accounts work before they buy them. Ransom demands from Dharma actors trend below those of the other major types of targeted ransomware over the past year. In December of 2019, when the average ransomware demand had surged to $191,000, the average Dharma ransom demand was only $8,620. That’s in part due to the types of targets hit by Dharma (mostly small and medium businesses), and in part because of the skills, experience and location of the affiliates running the attacks. In any case, Dharma operators make up for the lower ransom demands with volume—Dharma remains one of the most profitable ransomware families, according to Coveware.

Dharma uses a complicated two-stage decryption process that partitions the affiliate actors from the actual key retrieval process. Victims who contact the attackers are given a first-stage tool that extracts information about the files that were encrypted into a text file. That

text file gets cut-and-pasted into email and is sent back to the affiliates—who then have to submit that data through a portal for the RaaS to obtain the actual keys. This keeps the affiliates dependent on the RaaS, and it keeps them paying for service.

Just how well the decryption process works depends greatly on the expertise and the moods of the affiliates. Occasionally an actor will hold back some of the keys with additional demands. And there's constant "churn" among the front-end actors, as the "subscriptions" of some to RaaS services expire and others with less experience take their place, resulting in occasional misfires.

The Dharma playbook

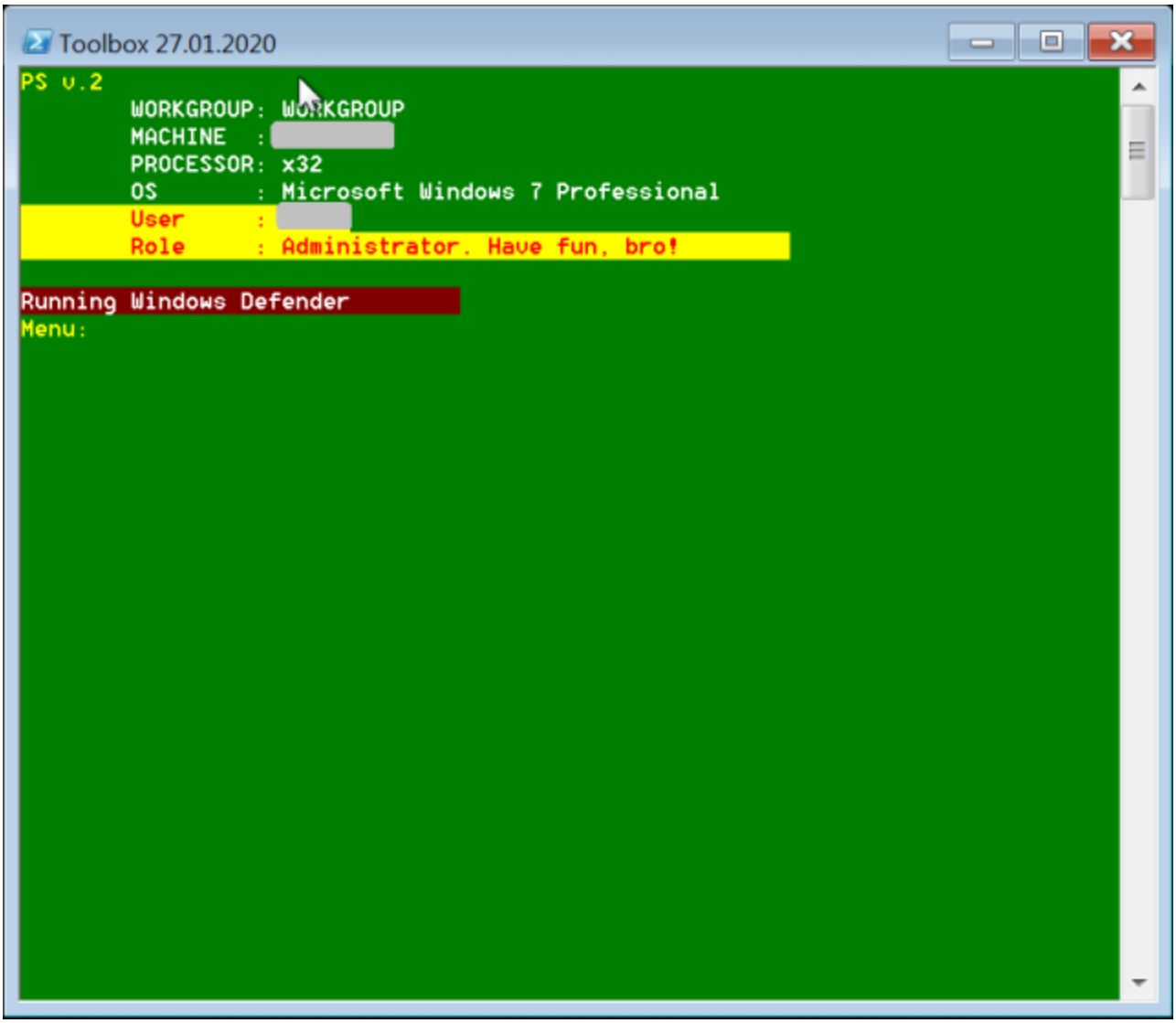
Most Dharma operators don't make significant changes to the source. But Dharma RaaS operators appear to package together a number of tools and best practices for their "affiliates" to use once they've gotten onto a victim's network.

These tools aren't completely automated, as every attack does not follow the same exact steps. However, they do follow something amounting to step-by-step instructions, akin to a telemarketer's script, allowing some room for improvisation. And one of those tools is a menu-driven PowerShell script that installs and launches the components required to spread ransomware across the network.

After getting an RDP connection, the attacker maps a directory containing the RaaS toolkit on their local drive as a network drive accessible from the remote desktop. The contents of this directory include a number of applications previously identified as potentially unwanted applications (such as the Mimikatz password extraction tool), customized hacking tools, and freeware versions of a variety of legitimate system utilities. (A full list of the files is included in the indicators of compromise file on SophosLabs' GitHub page.)

The kit also includes the Dharma ransomware executable, and a collection of PowerShell scripts, most of which we were unable to recover for analysis. However, we did recover a master script from console logs. Called toolbelt.ps1, the menu-driven console script automates the use of the tools, allowing attackers to simply type in the number associated with each pre-scripted element.

When executed, it identifies itself in the console frame as "Toolbox," and if executed with administrative privileges, advises the user/attacker, "Have fun, bro!"

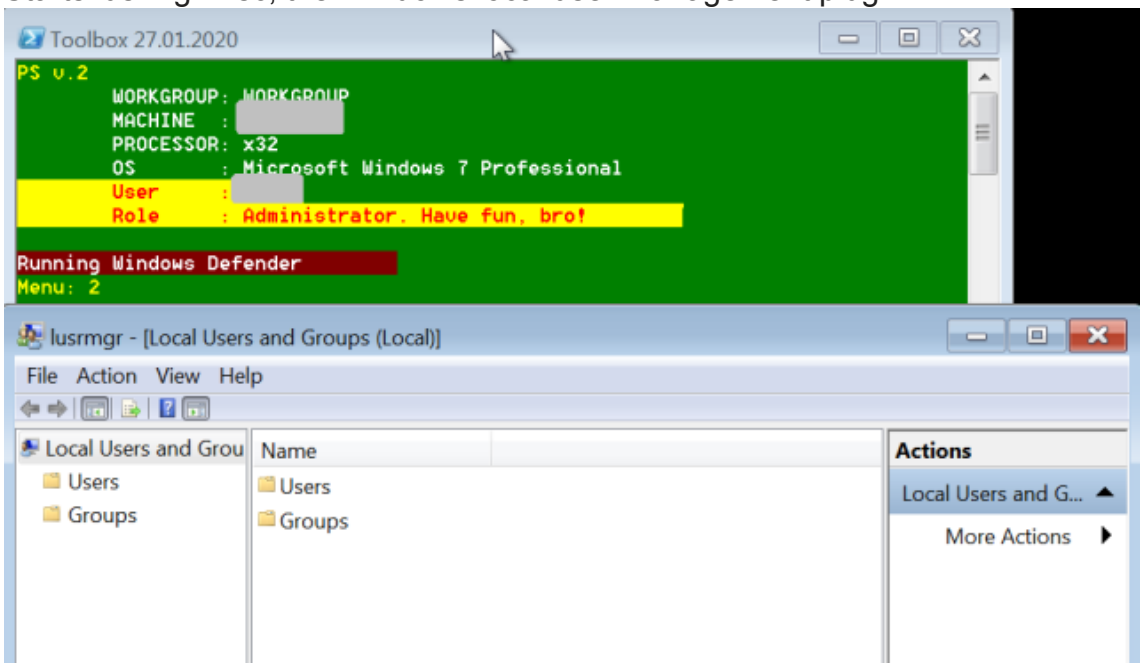


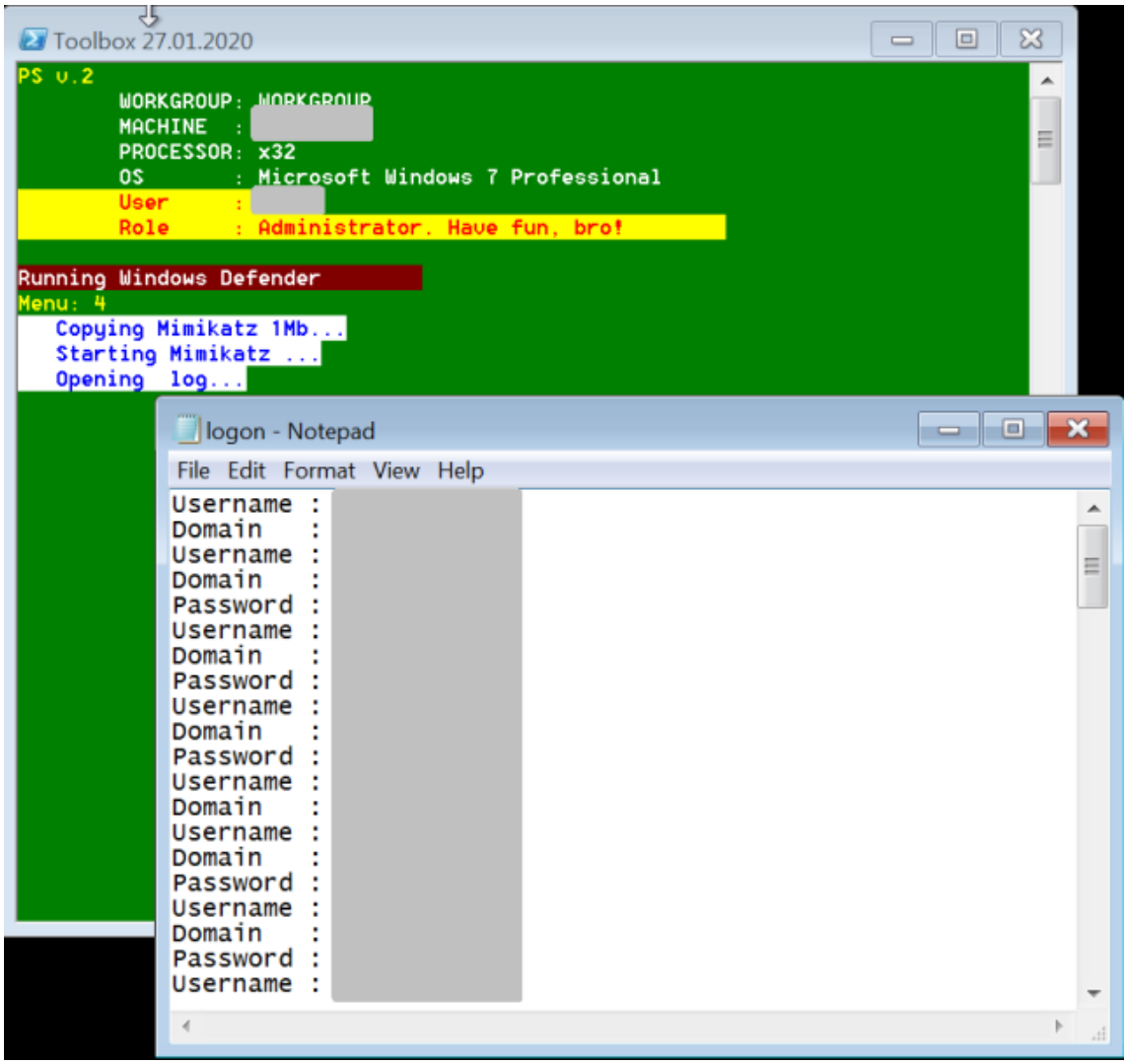
The startup screen for toolbelt.ps1

The “menu” selections in Toolbox aren’t displayed as a menu by the script as it executes, though they are largely documented in the script itself. Tools are downloaded to the remote computer by the script as needed, executed, and in many cases deleted after use.

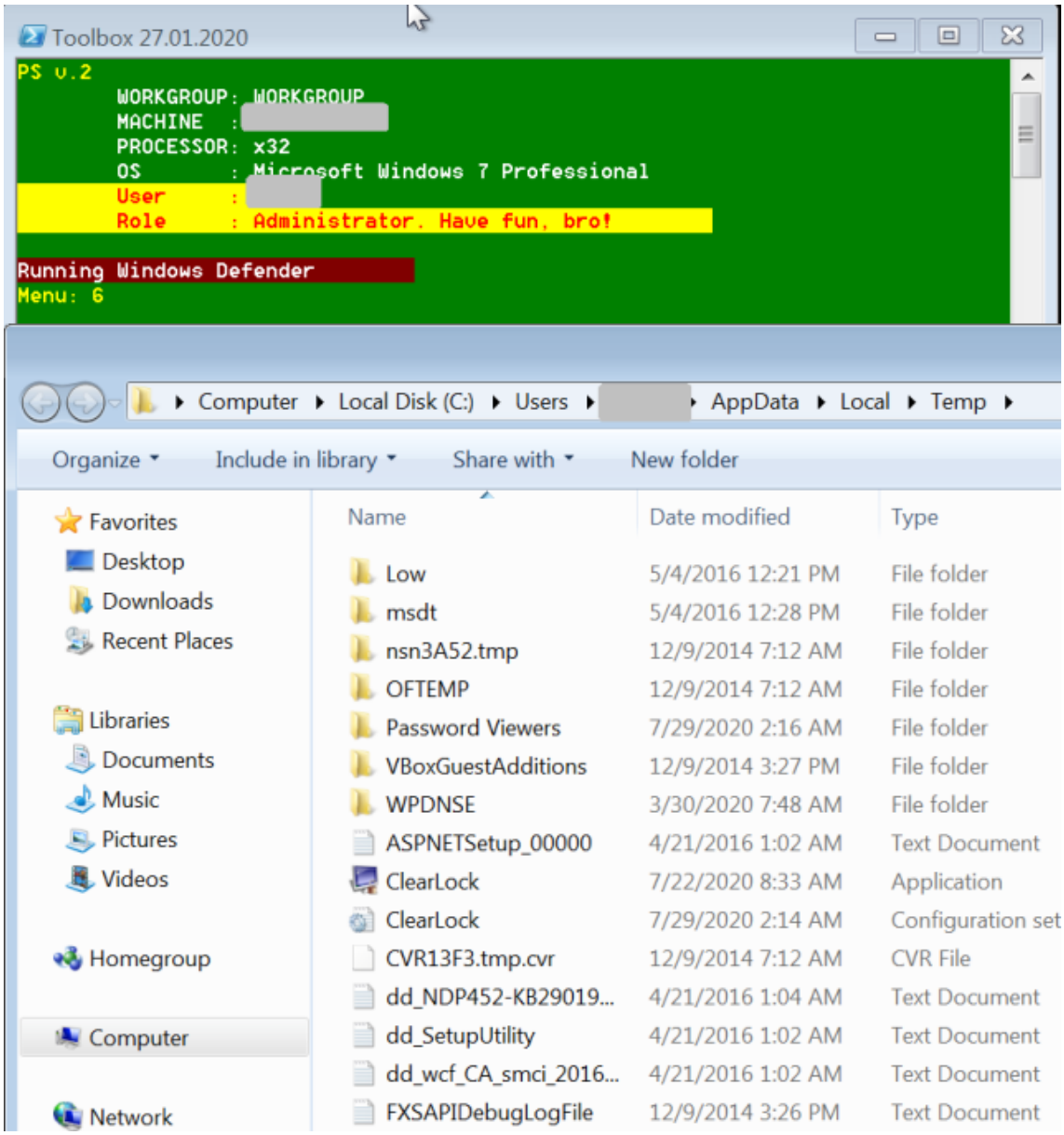
The menu commands we identified, by the numbers and symbols they are called by, were as follows:

“Menu” entry	**Triggered function**
+	Executes Start-Tor.ps1, a script that launches a Tor network connection.
.	Executes Email-Screenshot.ps1, which creates a screenshot from the remote system and sends to the email address (provided by the operator at a prompt in the script).
1	Runs LaPass.ps1, a “User changer” script. (We could not recover the script itself.)

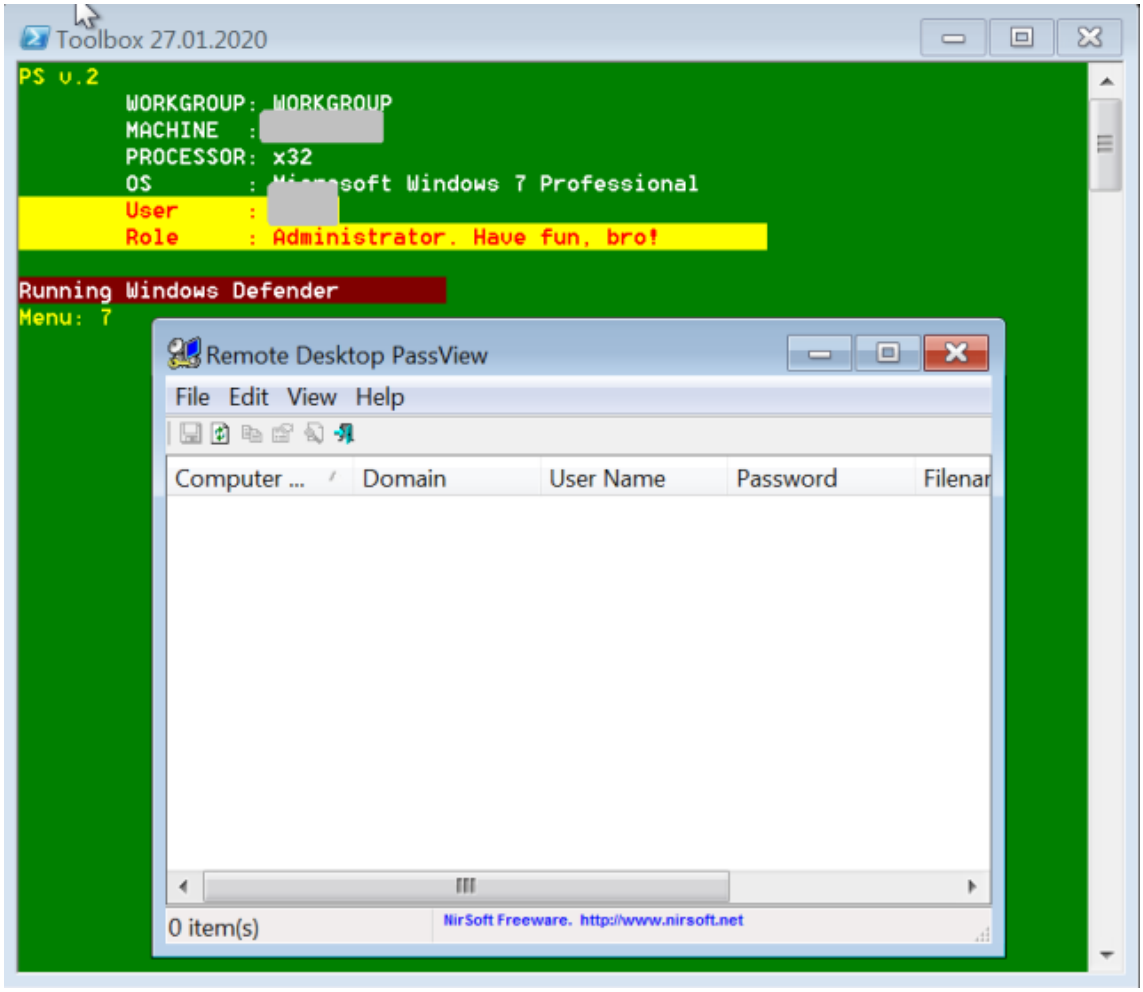
2	Starts lusrmgr.msc, the Windows local user management plug-in. 
3	Executes lubrute.ps1, a PowerShell script that attempts to get passwords to local user accounts through a brute force attack.
4	Copies and launches Mimikatz password extraction tools, dumping results to a text file.

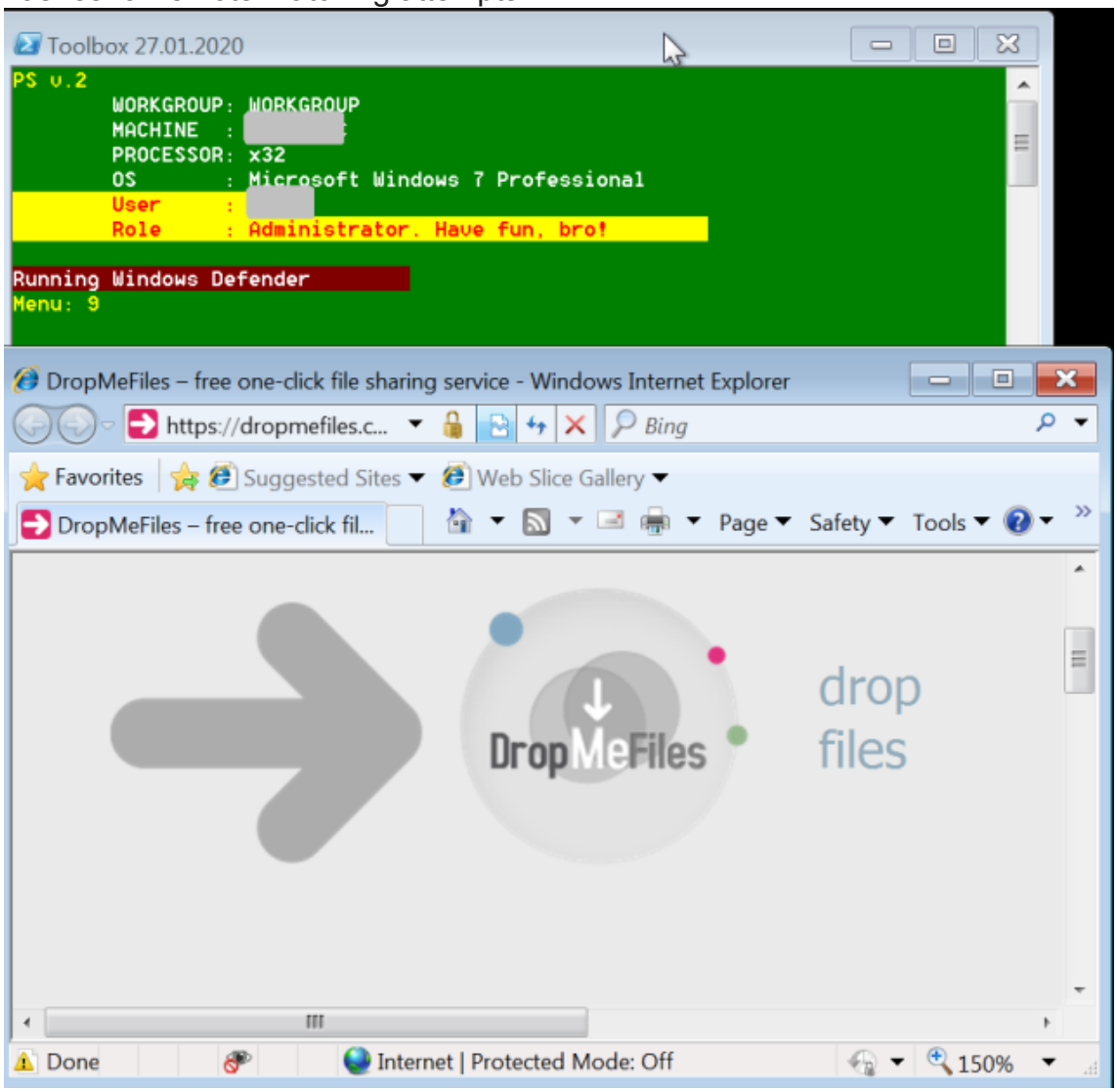


5	Executes Find-Pass.ps1, a PowerShell script. (We were unable to recover this script for analysis.)
6	Copies password viewers from a shared directory on the initially compromised machine to %temp%, and then opens a File Explorer window on that directory.

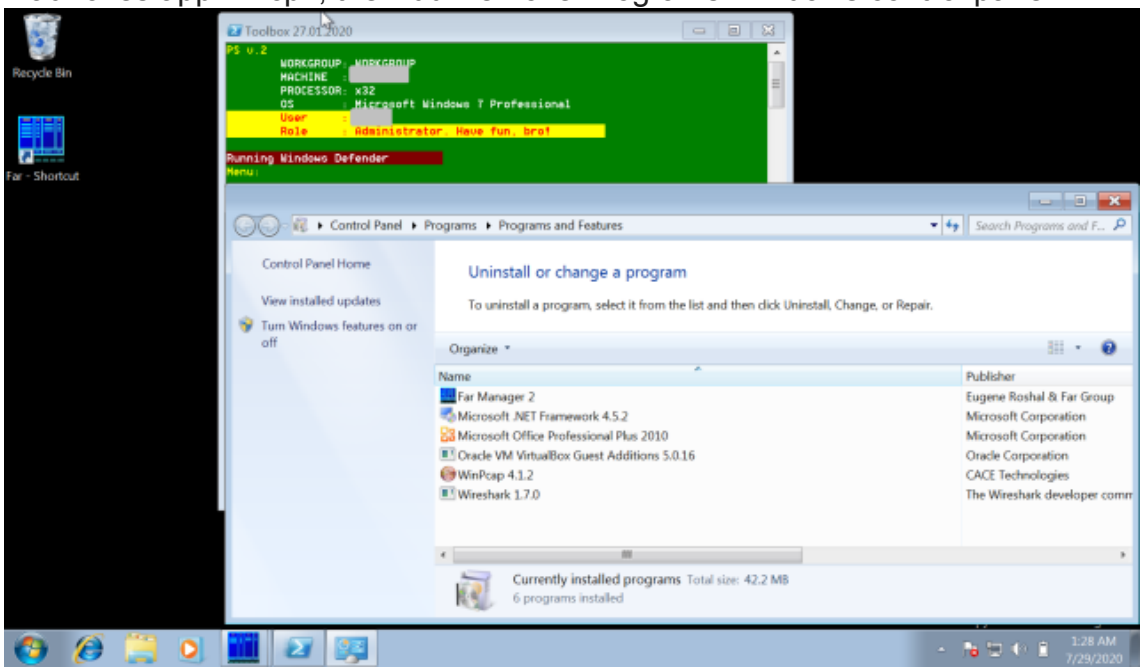

Toolbox 27.01.2020
PS v.2
WORKGROUP: WORKGROUP
MACHINE :
PROCESSOR: x32
OS : Microsoft Windows 7 Professional
User :
Role : Administrator. Have fun, bro!
Running Windows Defender
Menu: 6
Computer ▸ Local Disk (C:) ▸ Users ▸ AppData ▸ Local ▸ Temp ▸
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
Name
Date modified
Type
Low 5/4/2016 12:21 PM File folder
msdt 5/4/2016 12:28 PM File folder
nsn3A52.tmp 12/9/2014 7:12 AM File folder
OFTEMP 12/9/2014 7:12 AM File folder
Password Viewers 7/29/2020 2:16 AM File folder
VBoxGuestAdditions 12/9/2014 3:27 PM File folder
WPDNSE 3/30/2020 7:48 AM File folder
ASPNETSetup_00000 4/21/2016 1:02 AM Text Document
ClearLock 7/22/2020 8:33 AM Application
ClearLock 7/29/2020 2:14 AM Configuration set
CVR13F3.tmp.cvr 12/9/2014 7:12 AM CVR File
dd_NDP452-KB29019... 4/21/2016 1:04 AM Text Document
dd_SetupUtility 4/21/2016 1:02 AM Text Document
dd_wcf_CA_smci_2016... 4/21/2016 1:02 AM Text Document
FXSAPIDebugLogFile 12/9/2014 3:26 PM Text Document

6

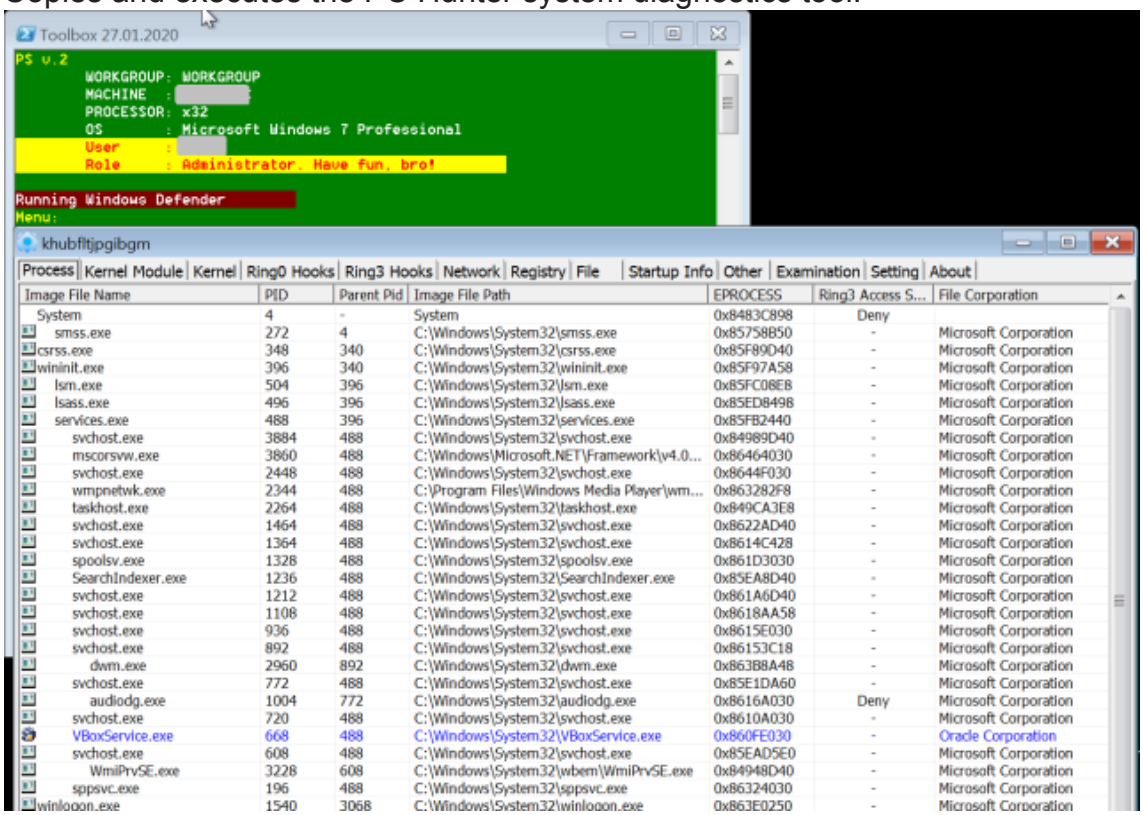
7	Copies and and executes the NirSoft Remote Desktop PassView password viewer tool. 
8	Copies and executes LaZagne.exe, the Windows executable version of the LaZagne password scraper.

9	Copies and executes Hash Suite Tools Free edition's Hash Dump utility, and opens the website dropmefiles[.]com—potentially to exfiltrate the password hashes for remote matching attempts. 
10	Runs the script Delete-AVServices.ps1, which searches a list of malware protection related Windows services and partial service names to search for and kill.

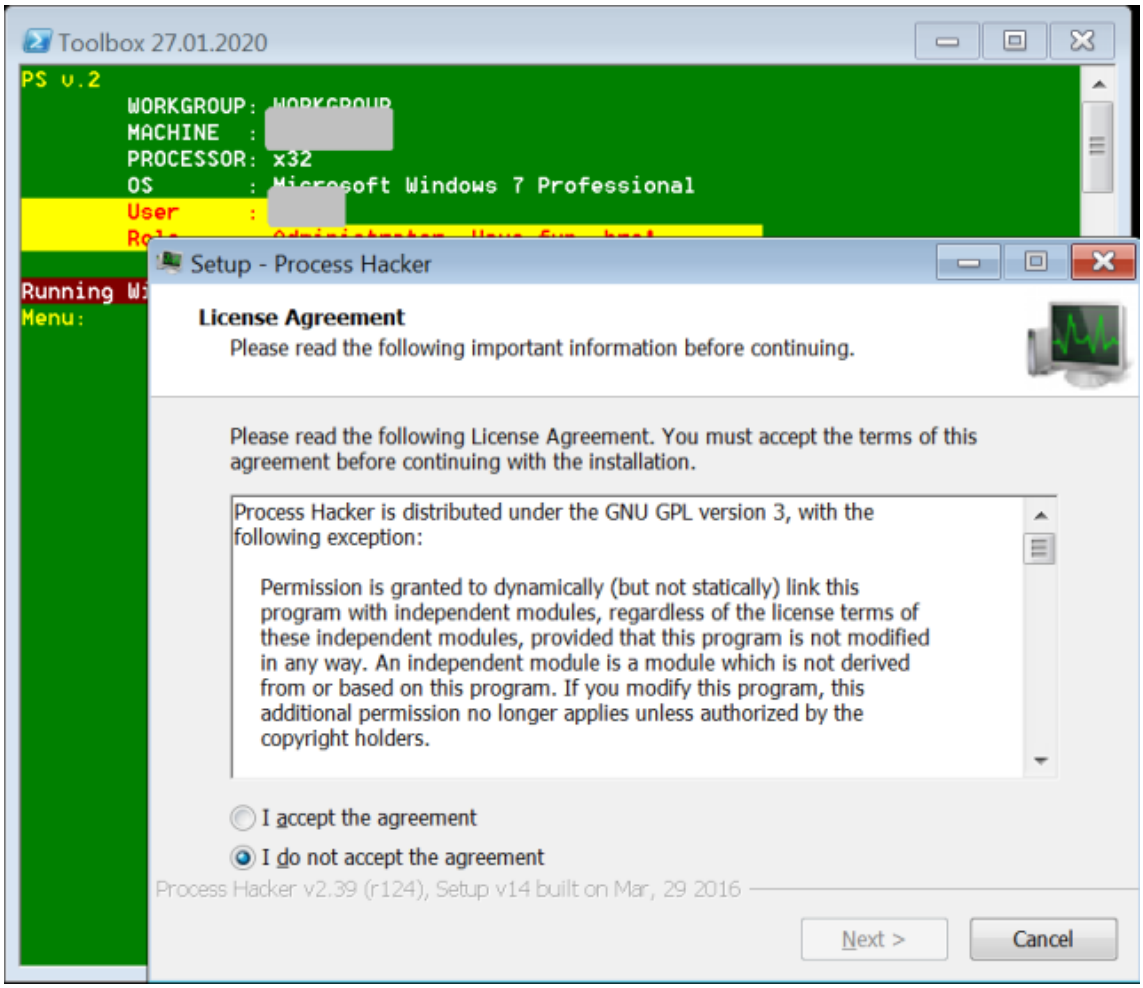
11 Launches appwiz.cpl , the Add/Remove Programs Windows control panel.

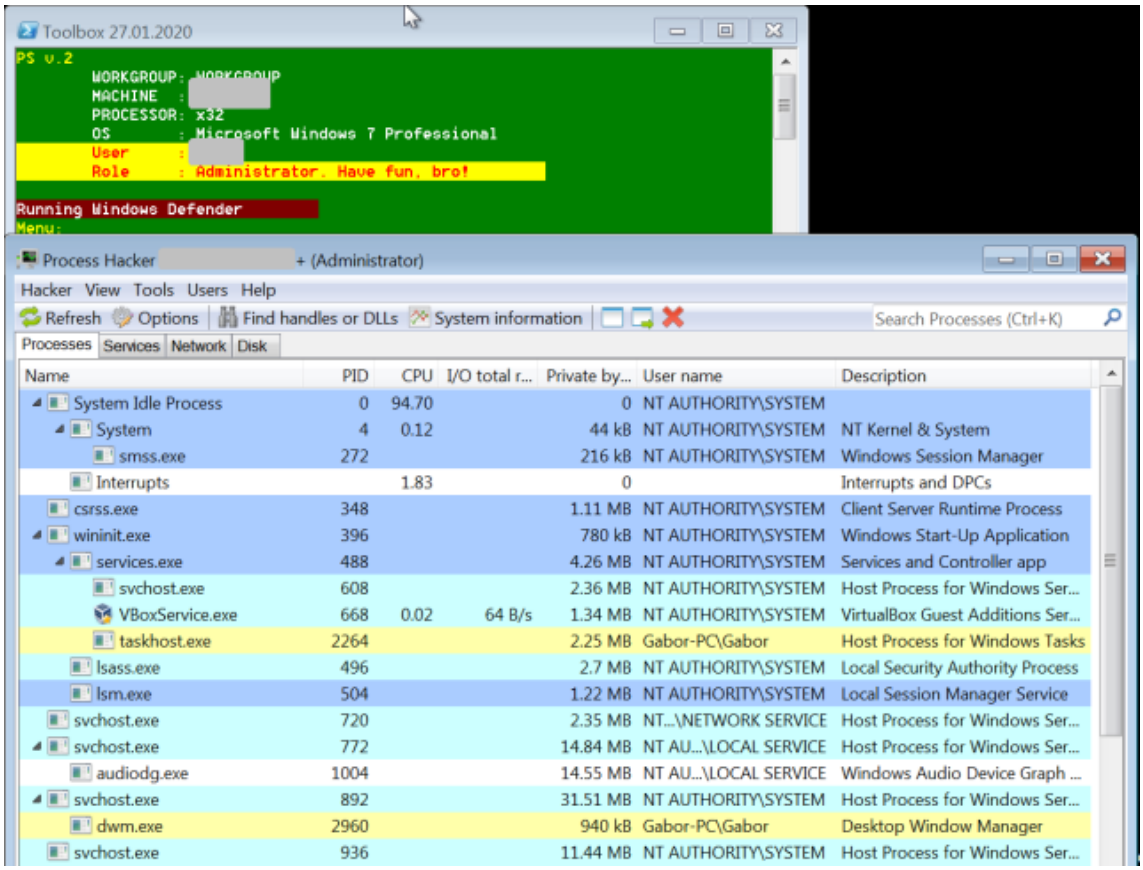


12 Copies and executes the PC Hunter system diagnostics tool.

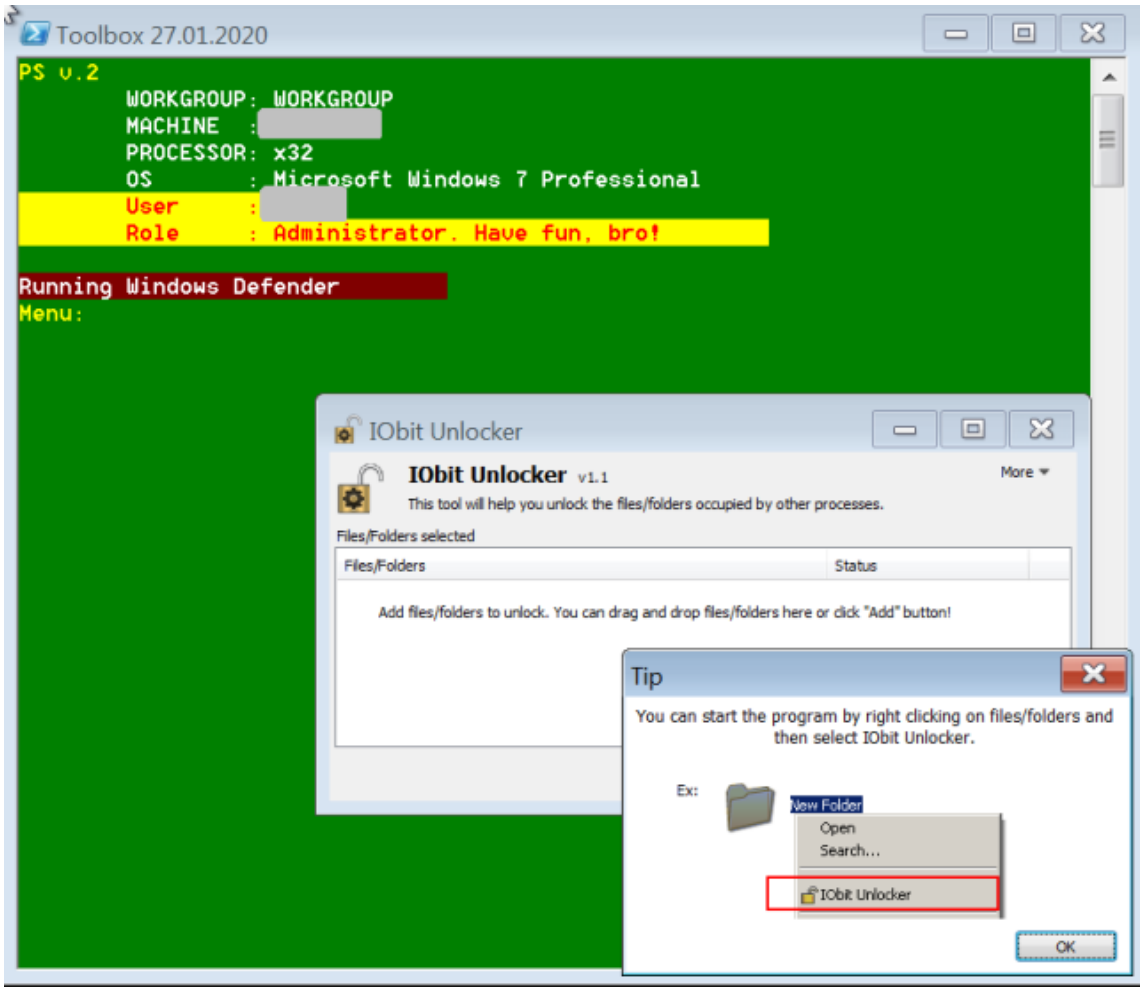


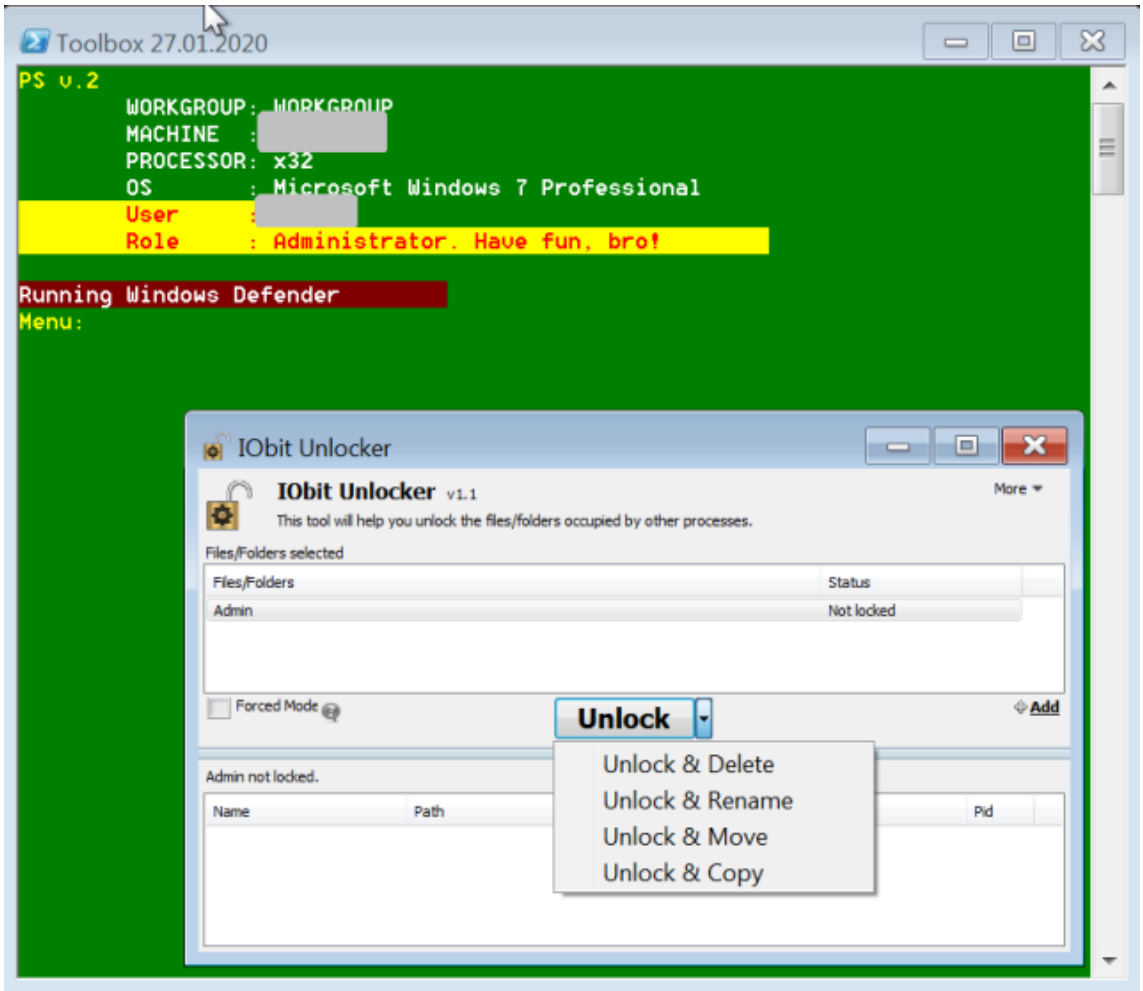
13 Copies, installs and executes ProcessHacker:


Toolbox 27.01.2020
PS v.2
WORKGROUP: WORKGROUP
MACHINE :
PROCESSOR: x32
OS : Microsoft Windows 7 Professional
User :
Running W
Menu:
Setup - Process Hacker
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
Process Hacker is distributed under the GNU GPL version 3, with the following exception:
Permission is granted to dynamically (but not statically) link this program with independent modules, regardless of the license terms of these independent modules, provided that this program is not modified in any way. An independent module is a module which is not derived from or based on this program. If you modify this program, this additional permission no longer applies unless authorized by the copyright holders.
I accept the agreement
I do not accept the agreement
Process Hacker v2.39 (r124), Setup v14 built on Mar, 29 2016
Next >
Cancel

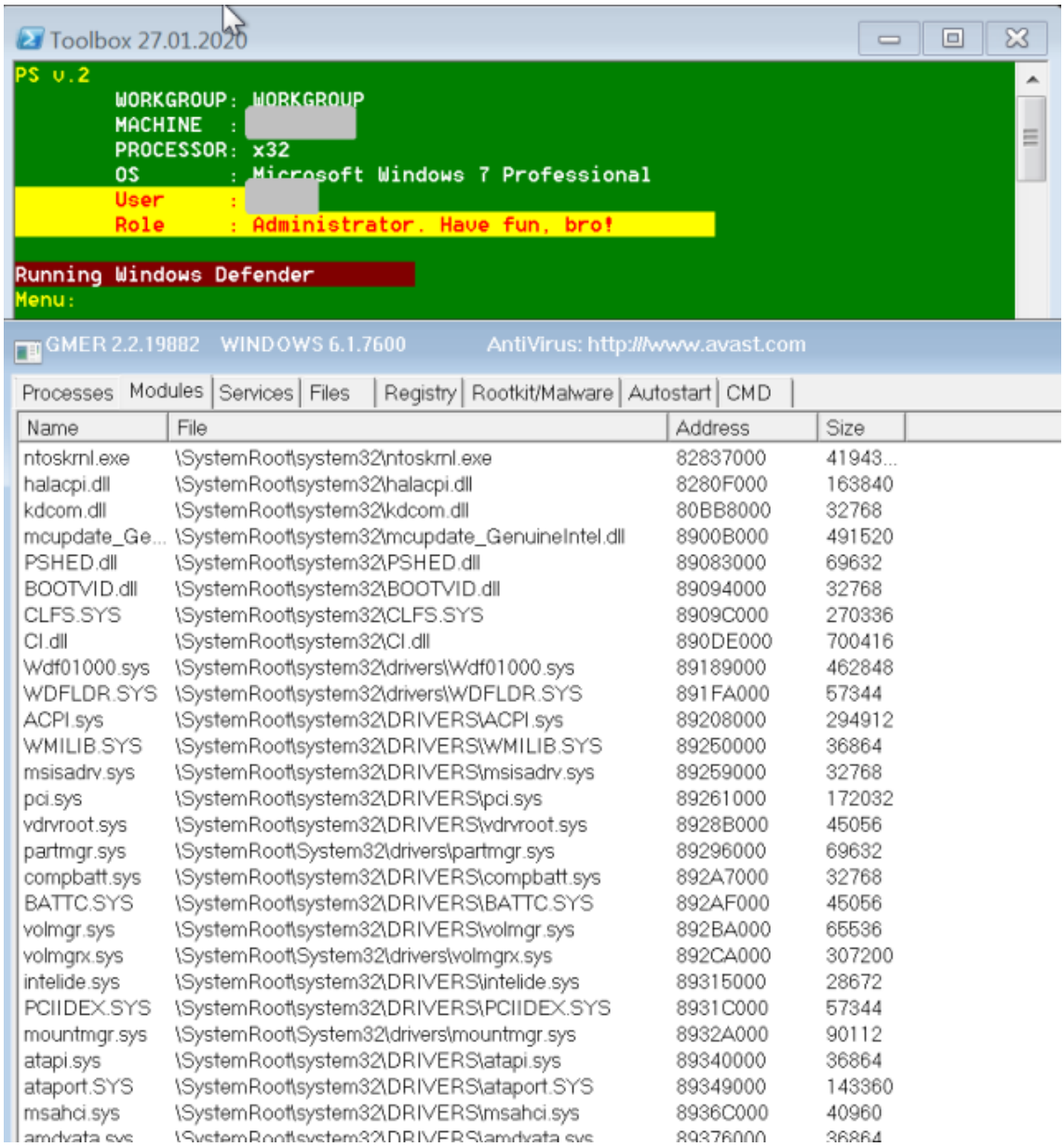

Toolbox 27.01.2020
PS v.2
WORKGROUP: WORKGROUP
MACHINE :
PROCESSOR: x32
OS : Microsoft Windows 7 Professional
User :
Role : Administrator. Have fun, bro!
Running Windows Defender
Menu:
Process Hacker + (Administrator)
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Processes (Ctrl+K)
Processes Services Network Disk
Name PID CPU I/O total r... Private by... User name Description
System Idle Process 0 94.70 0 NT AUTHORITY\SYSTEM
System 4 0.12 44 kB NT AUTHORITY\SYSTEM NT Kernel & System
smss.exe 272 216 kB NT AUTHORITY\SYSTEM Windows Session Manager
Interrupts 1.83 0 Interrupts and DPCs
csrss.exe 348 1.11 MB NT AUTHORITY\SYSTEM Client Server Runtime Process
wininit.exe 396 780 kB NT AUTHORITY\SYSTEM Windows Start-Up Application
services.exe 488 4.26 MB NT AUTHORITY\SYSTEM Services and Controller app
svchost.exe 608 2.36 MB NT AUTHORITY\SYSTEM Host Process for Windows Ser...
VBoxService.exe 668 0.02 64 B/s 1.34 MB NT AUTHORITY\SYSTEM VirtualBox Guest Additions Ser...
taskhost.exe 2264 2.25 MB Gabor-PC\Gabor Host Process for Windows Tasks
lsass.exe 496 2.7 MB NT AUTHORITY\SYSTEM Local Security Authority Process
lsm.exe 504 1.22 MB NT AUTHORITY\SYSTEM Local Session Manager Service
svchost.exe 720 2.35 MB NT...\NETWORK SERVICE Host Process for Windows Ser...
svchost.exe 772 14.84 MB NT AU...\LOCAL SERVICE Host Process for Windows Ser...
audiodg.exe 1004 14.55 MB NT AU...\LOCAL SERVICE Windows Audio Device Graph ...
svchost.exe 892 31.51 MB NT AUTHORITY\SYSTEM Host Process for Windows Ser...
dwm.exe 2960 940 kB Gabor-PC\Gabor Desktop Window Manager
svchost.exe 936 11.44 MB NT AUTHORITY\SYSTEM Host Process for Windows Ser...

14 Copies, installs and executes IOBit Unlocker, a utility for removing file locks that would prevent deletion or encryption,

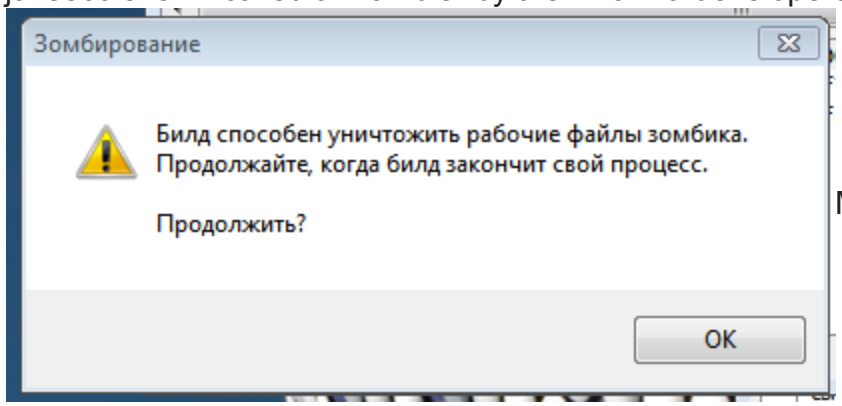

Toolbox 27.01.2020
PS v.2
WORKGROUP: WORKGROUP
MACHINE :
PROCESSOR: x32
OS : Microsoft Windows 7 Professional
User :
Role : Administrator. Have fun, bro!
Running Windows Defender
Menu:
IObit Unlocker
IObit Unlocker v1.1
More
This tool will help you unlock the files/folders occupied by other processes.
Files/Folders selected
Files/Folders
Status
Add files/folders to unlock. You can drag and drop files/folders here or click "Add" button!
Tip
You can start the program by right clicking on files/folders and then select IObit Unlocker.
Ex:
New Folder
Open
Search...
IObit Unlocker
OK



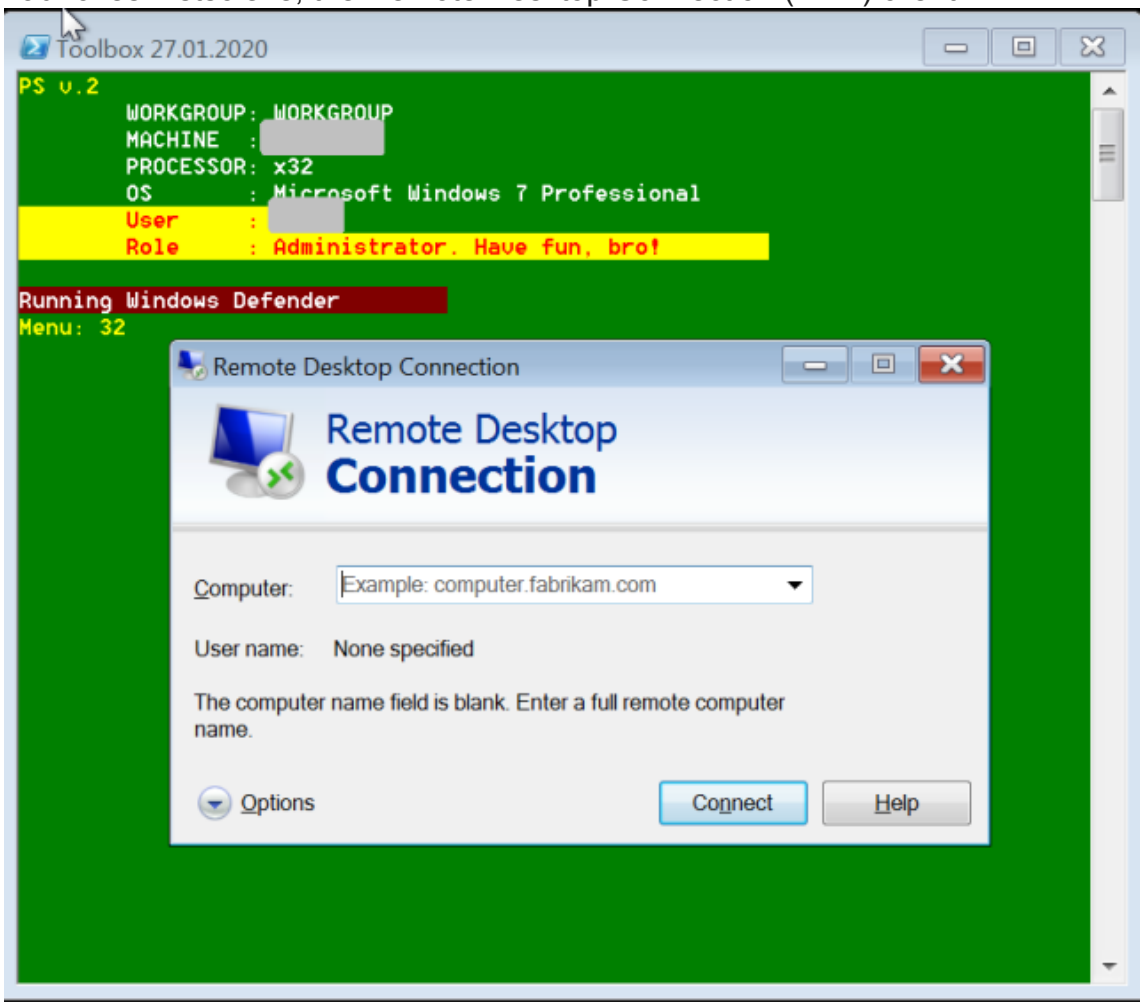
15	Copies and executes GMER, a “rootkit detector” used to reveal hidden processes.



16	Copies and executes a freeware version of Revo Uninstaller, a tool for uninstalling Windows software and cleaning up files left over from an uninstall.
17	Copies and executes IOBit Uninstaller, another software uninstaller tool.
18	Executes a PowerShell script, “Disable-WinDefend.ps1 /t” .
20	Executes a PowerShell script, “purgeMemory.ps1/” .
21	Executes takeaway.exe , the payload package that drops the ransomware.
22	Stops the winhost.exe process (the Dharma ransomware executable)
23	Executes a PowerShell script, winhostok.ps1.

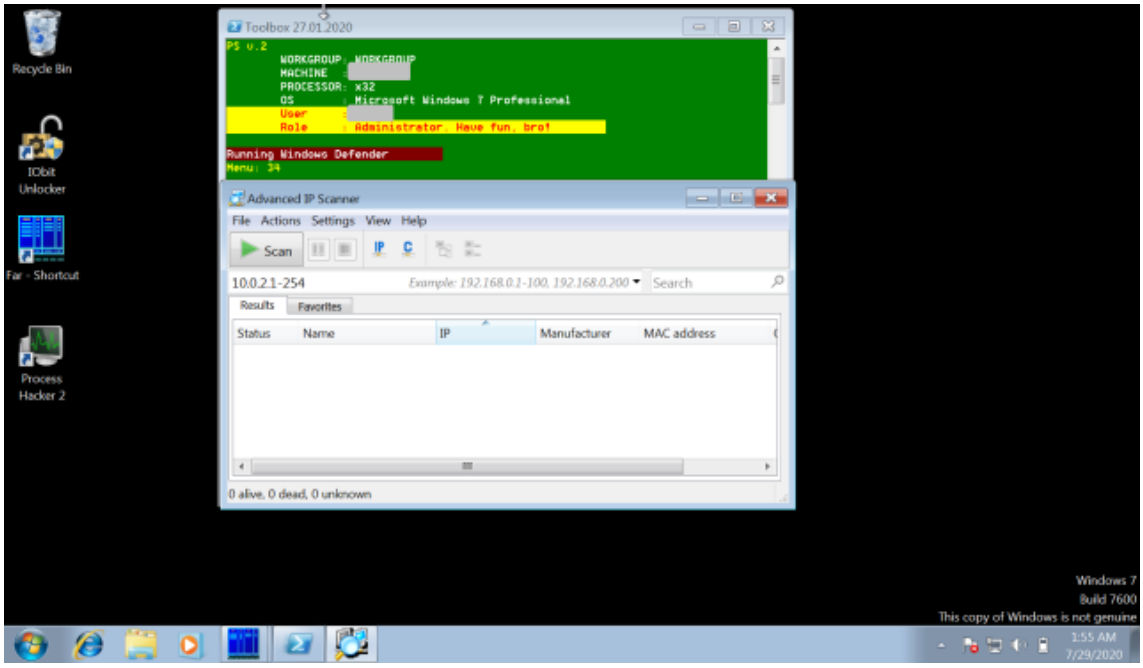
25	Calls a function of the script called “Infect”, which deploys a file called javsecc.exe — called a “zombie” by the Dharma developers.  Message box from javsecc.exe Upon execution, a message box pops up (the window name translates as “Zombification”). The message reads: *This build is able to destroy the working files of the “zombie”. Continue, when build process is finished. Continue?* Clicking “OK” executes an AutoIT process that: • obtains the external IP address of the system it runs on by calling multiple remote services: LOCAL $AGETIPURL = [“https://api.ipify.org” , “http://checkip.dyndns.org” , “http://www.myexternalip.com/raw” , “http://bot.whatismyipaddress.com”] • downloads and installs a Tor network client (tor.exe) ; • checks install of Tor by pinging the local host address, then deletes temporary files; • collects system information and user account data, and sends to a remote .onion (Tor) server. • sleeps and waits for timer events.
30	Executes a PowerShell script described as “Local Network Computer Listing” by the console output, called NetPC.ps1.
31	Executes the PowerShell script NetSubPC.ps1, another network computer name browser.

32	Launches mstsc.exe, the Remote Desktop Connection (RDP) client.



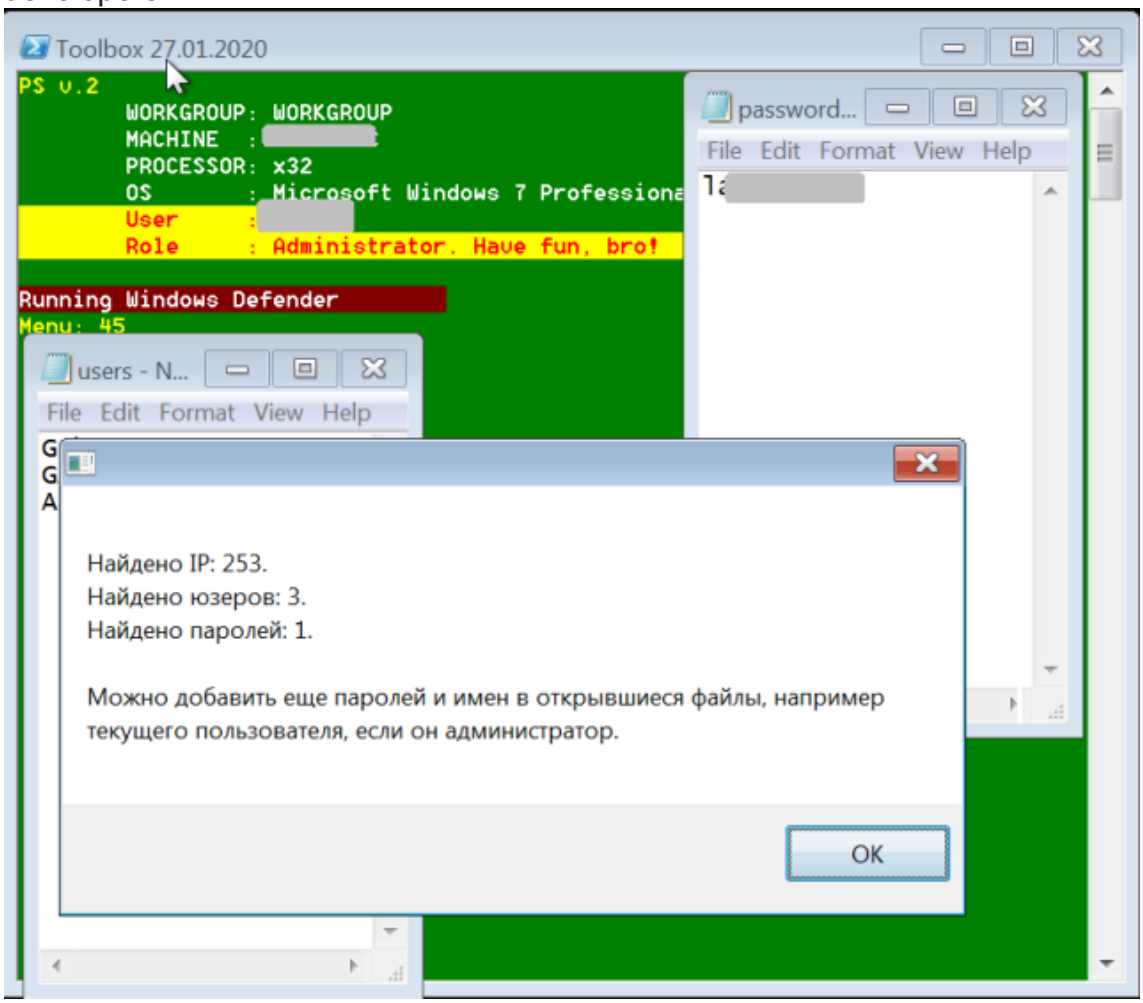
33	Copies and starts ns2.exe, a known PUA. The executable can scan for network shares and local unmounted volumes.

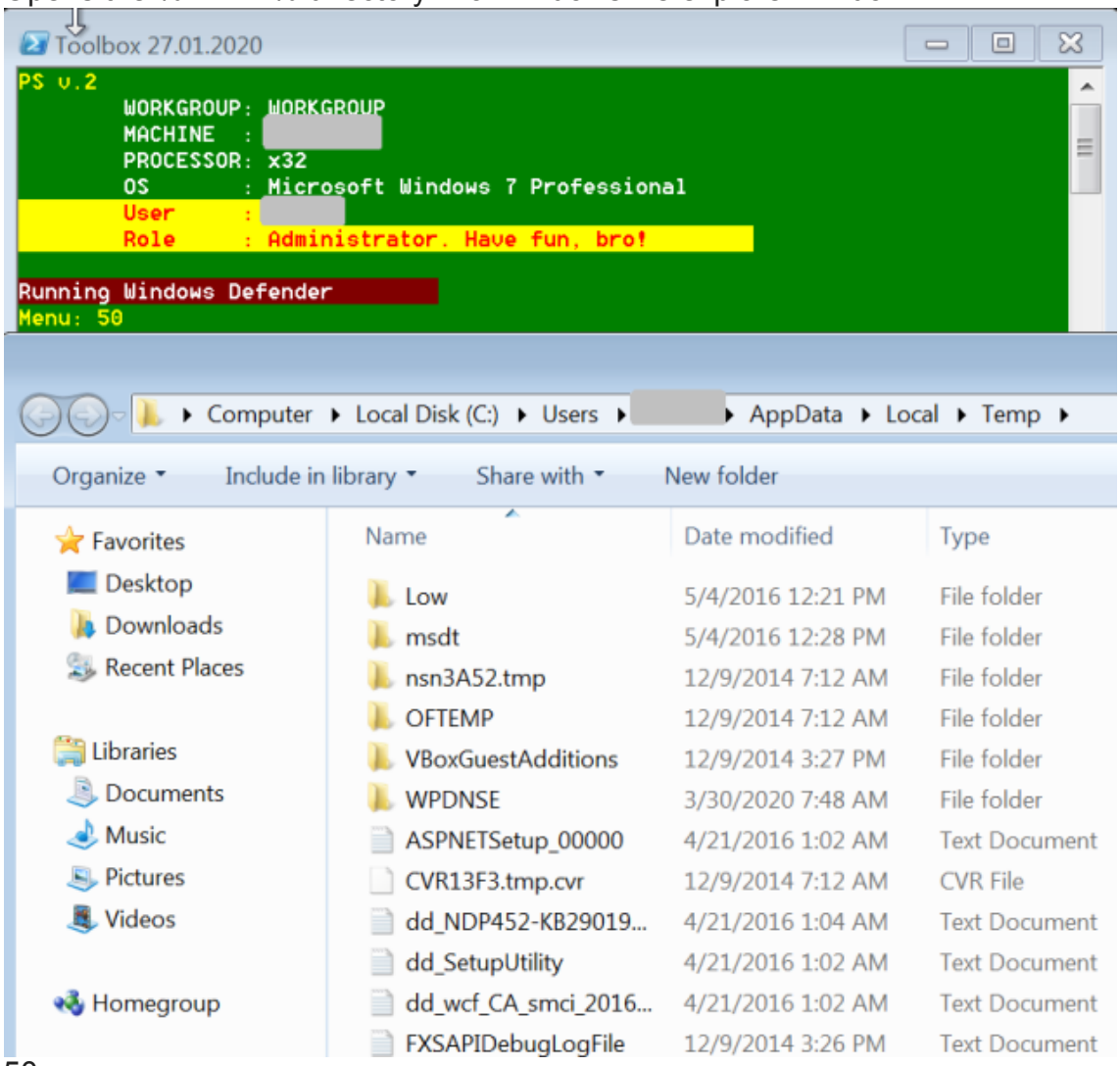
34	Copies and starts Advanced IP Scanner (IPScan2.exe), a commercial freeware tool that can identify and access shared network folders, control other computers on the network via RDP and Radmin remote control software, and execute remote shutdowns.



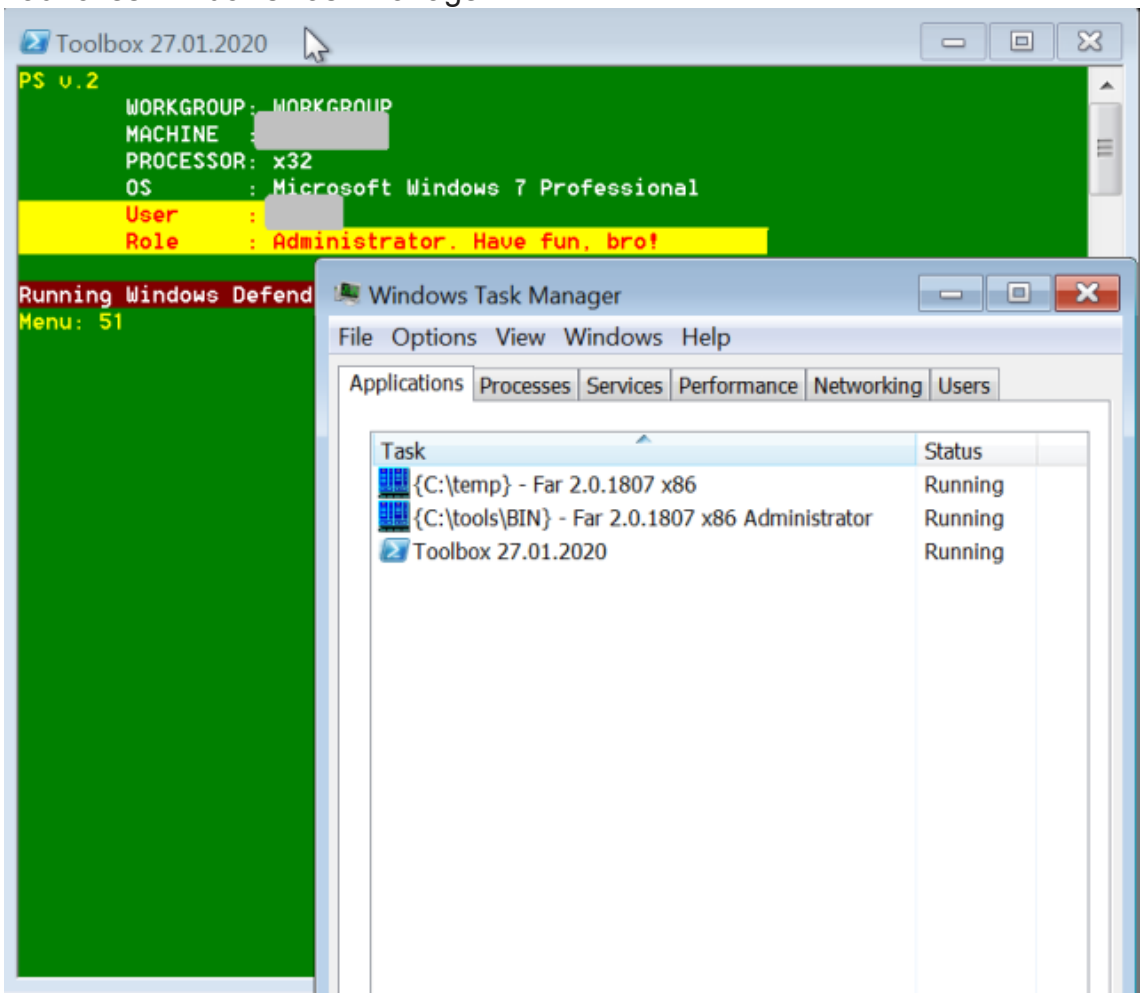
40	Retrieves a list of computers from Active Directory by running NetADPC.ps1.
41	Executes a PowerShell script named adbrute.ps1 (likely another Mimikatz scripted brute force attack on Active Directory accounts).
42	Copies and executes a PowerShell script named 2sys.ps1.
43	Launches the Windows Active Directory management snap-in (dsa.msc).
44	Launches the Group Policy Management Console snapin (gpmc.msc).

45 Runs “Mimi NL,” a more automated version of the Mimikatz password hacking tool. This tool appears to have been developed by the Dharma RaaS developers.



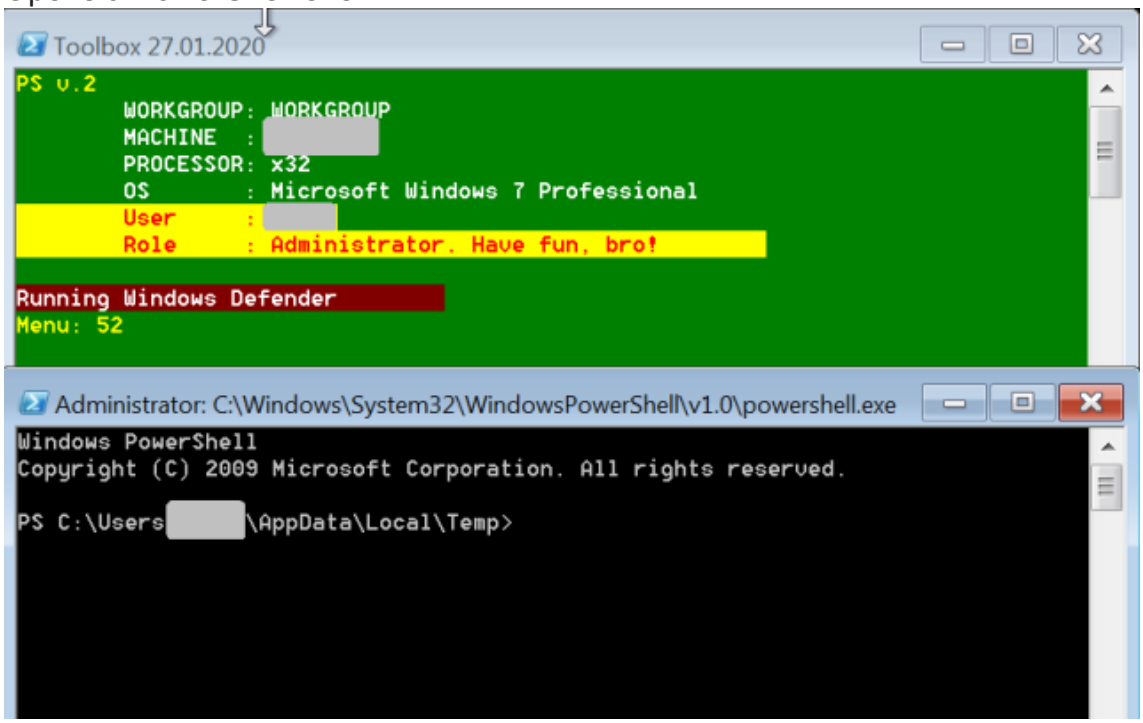
50	Opens the %TEMP% directory in a Windows file explorer window.  50

51 Launches Windows Task Manager.



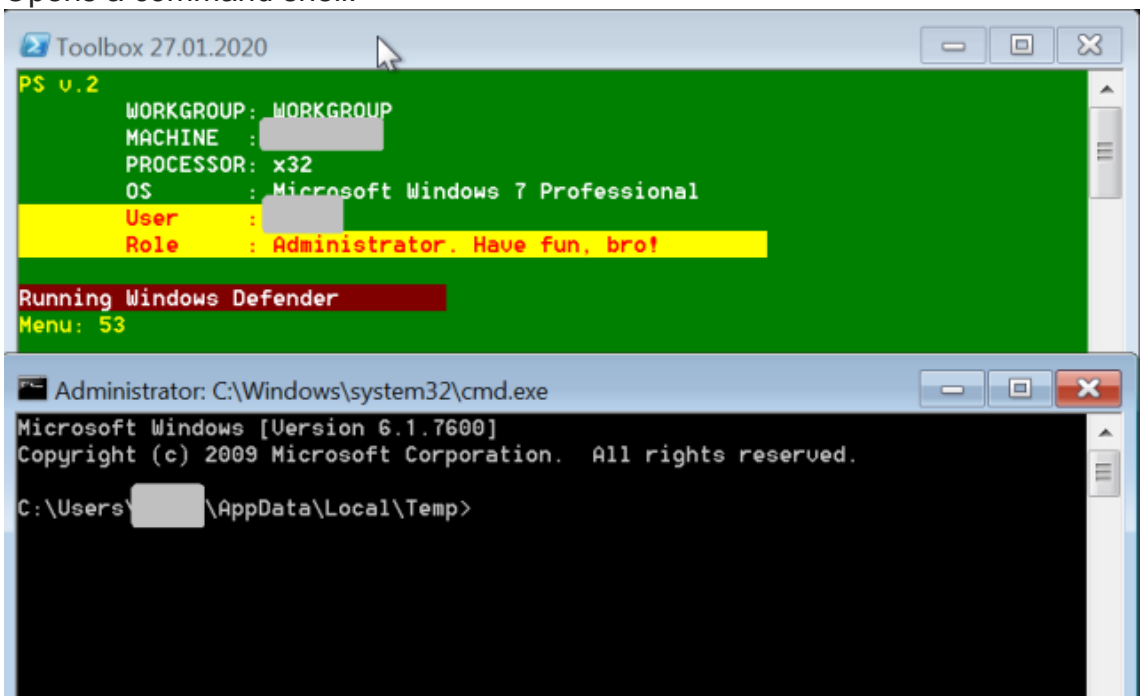
51

52	Opens a PowerShell shell.

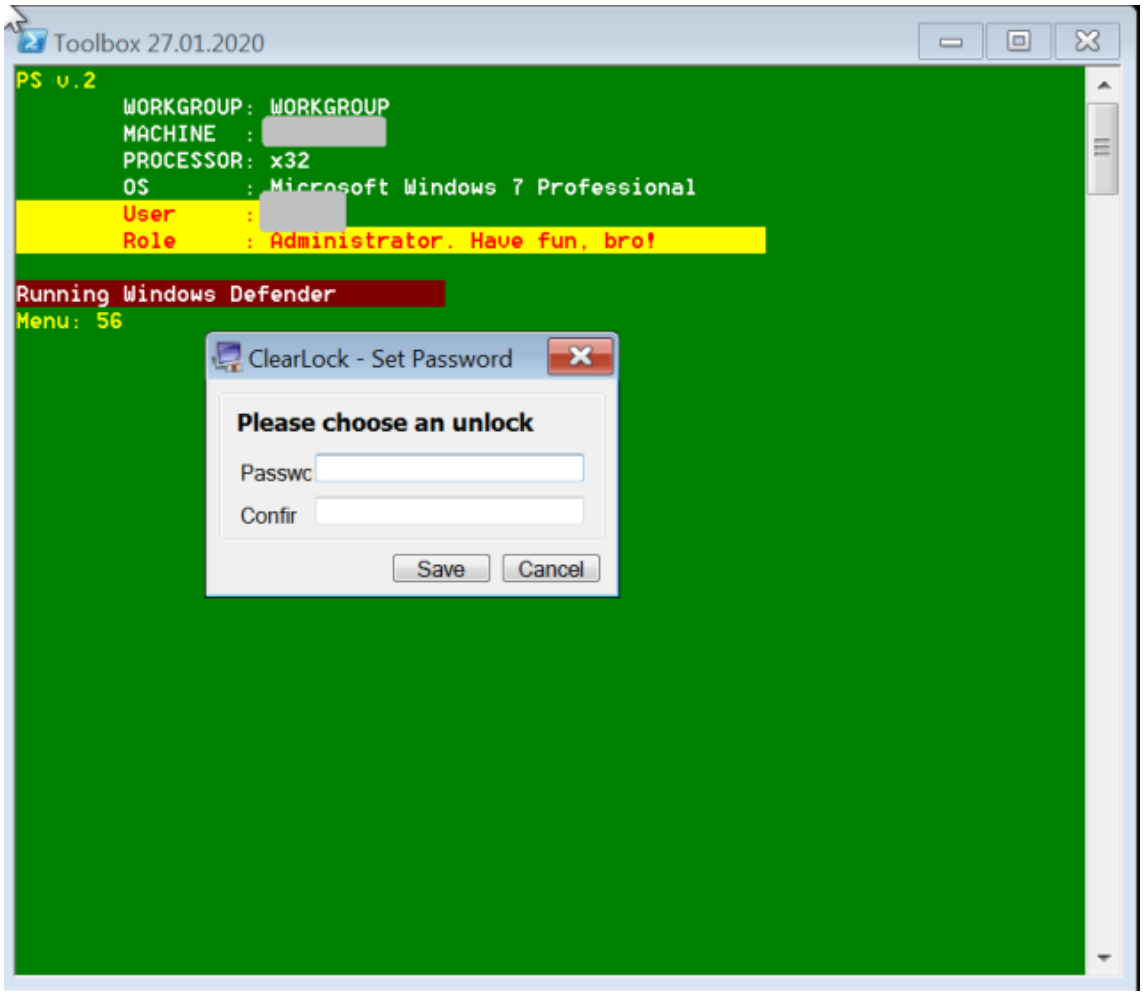


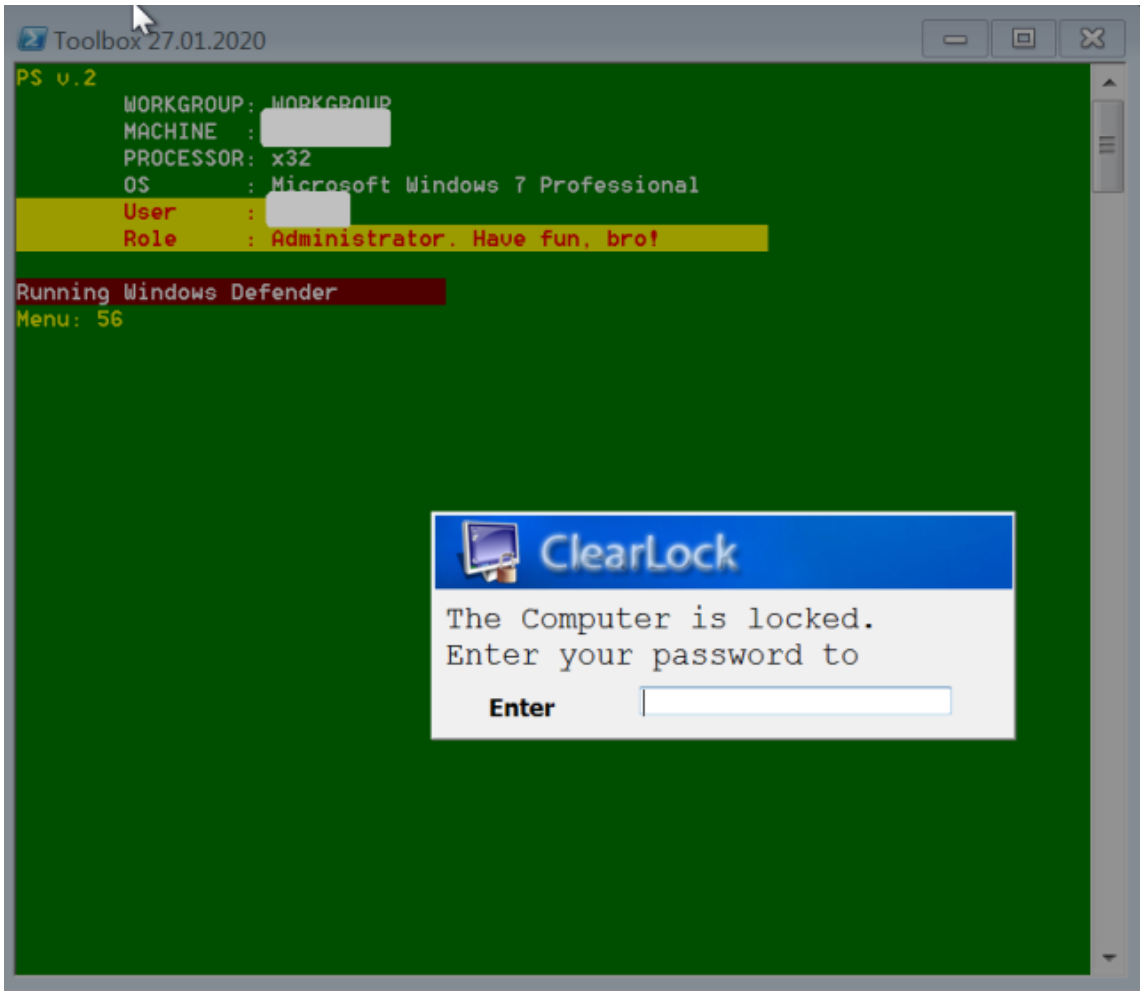
52

53	Opens a command shell.



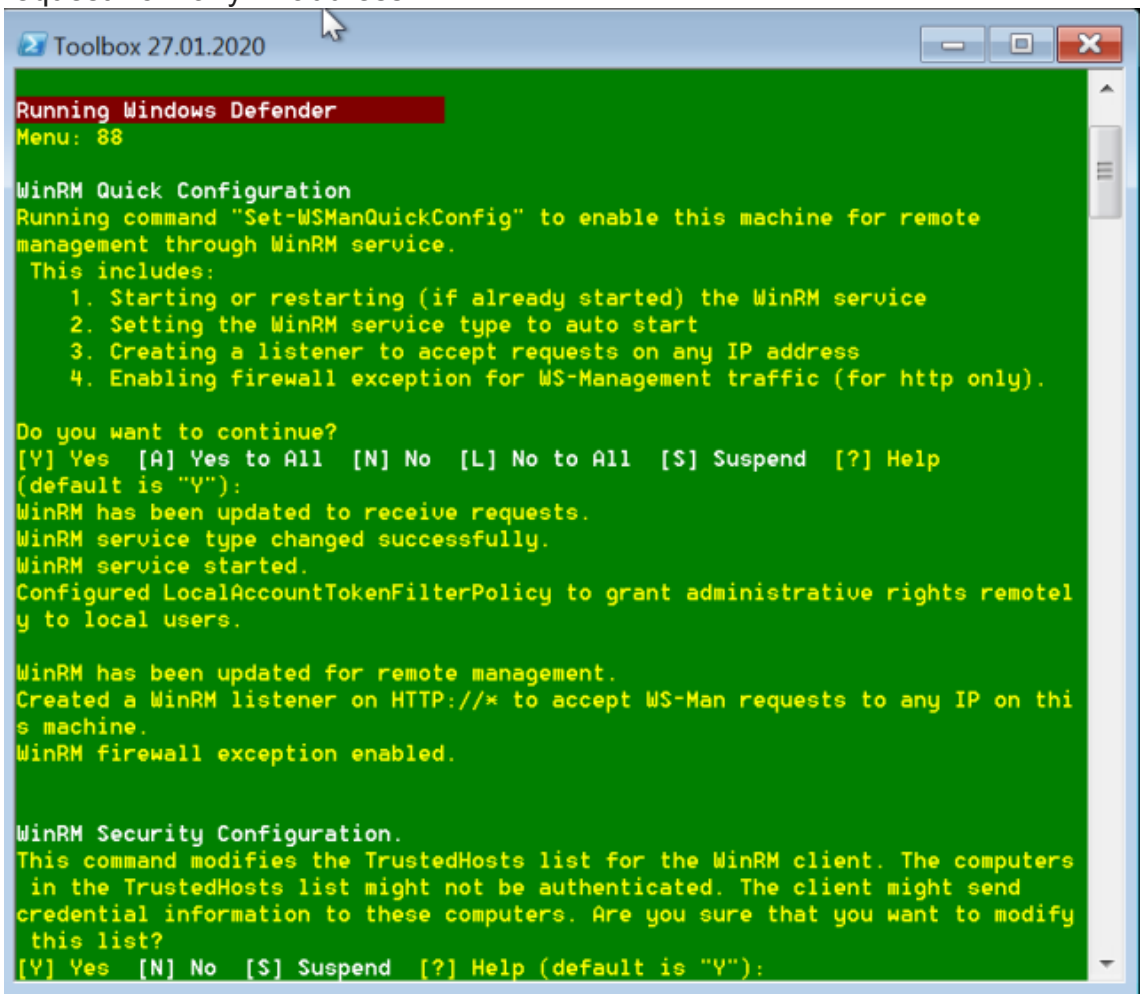
54	Runs rdclip.exe, the Remote Desktop shared clipboard.
55	Reboots the computer.
56	Copies and executes ClearLock.exe, a screen locker.


Toolbox 27.01.2020
PS v.2
WORKGROUP: WORKGROUP
MACHINE :
PROCESSOR: x32
OS : Microsoft Windows 7 Professional
User :
Role : Administrator. Have fun, bro!
Running Windows Defender
Menu: 56
ClearLock - Set Password
Please choose an unlock
Passwc
Confir
Save
Cancel



57	Executes a PowerShell script called wallet.ps1.
60	Copies and executes a batch script, addSupport.bat.
61	Copies and executes a published proof-of-concept privilege escalation exploit (CVE-2018-8120) —either the 32-bit (x86.exe) or 64-bit (x64.exe) version.
99	Starts toolbelt1.ps1 (which could be updated version of toolbelt).

88	Enables WinRM remote management using the WS-Management protocol, This allows administrative commands to be sent to the computer via an HTTP request from any IP address.



101	Copies and executes a program called SafeMode, launched with a batch script called AsAdmin.bat. (We did not recover these files for analysis.)
155	Copies and executes Registry Finder, a tool for editing Windows' Registry.
211	Copies and executes the Dharma payload package from the path mapped to the attacker's computer: $tsclient\x\1\Takeaway.exe.
212	Copies and executes the Dharma payload package from the path $tsclient\x\2\Takeaway.exe.
213	Copies and executes the Dharpayload package from the path $tsclient\x\3\Takeaway.exe.
214	Copies and executes payload package from the path $tsclient\x\4\Takeaway.exe.

222	Copies and executes javsec.exe, another automated Mimikatz password cracking tool built with AutoIT. The executable runs mimikatz.exe and a disguised version of the NL Brute utility named postgresqlapi.exe (a network login brute force tool).
223	Opens the directories $env\temp\$guid and $env\appdata\PostgreSQL\API\$guid (probably for temporary storage)
224	Performs “cleanup” by deleting processes tor, torque, and PostGreSQLapi.exe, and clears the directories $envtemp\$guid and $env\appdata\PostgreSQL\API\$guid.
300	Unpacks and executes the contents of the package LBru4v4.zip
401	Copies a directory called “WMIDomain” from the toolset share and executes a PowerShell script called GetHosts.ps1.
600	Kills all processes except for PowerShell and unnamed windows.

666	Executes a PowerShell command that writes a new script called “sample.ps1” from the contents of the Windows clipboard. That script is then executed in opens a command shell with the permissions of an account passed to the script with an environmental variable and a password encoded into the command opening the PowerShell shell (2qaz!QAZ).
	`{try {Add-Type -AssemblyName PresentationCore`
	`$clip = [Windows.Clipboard]::GetText()`
	`$clip | Out-File $destination\sample.ps1}`
	`catch {RedAlert Failed to copy vicious code. Try 52, then right click...}`
	`start  $PsHome\powershell.exe " -NoProfile -ExecutionPolicy Bypass -File $destination\sample.ps1" -Verb RunAs }`
	`- {start -FilePath cmd.exe -ArgumentList "/c net user $env:USERNAME 2qaz!QAZ & pause"}`
	The pasted code executes Takeaway.exe, the Dharma payload. If the code creation fails, the script advises the attacker to use menu entry 52 to respawn PowerShell.

The order of the use of the toolbelt.ps1 script varies, but we have observed common patterns among Dharma attackers. In one typical attack, we saw the operators follow the following steps:

- The attacker launched the toolbelt script (toolbelt.ps1 -it 1)
- 10: delete-avservices.ps1
- 15: GMER (gamer.exe)
- 13: installing and launching ProcessHacker
    - executing processhacker-2.39-setup.exe
    - executing processhacker.exe
- 222: javsec.exe (Mimikatz /NL Brute wrapper)

- 34: ipscan2.exe (Advanced IP Scanner)
- 32: mstsc.exe
- 21: takeaway.exe (ransomware package)
    - executes winhost.exe (Dharma)
    - executes purgememory.ps1
- 33: ns2.exe (network scan)

Playing by the book

While the toolbelt.ps1 script is somewhat self-documenting, it's clear that the end users of the script—the Dharma affiliates—are also operating from some other form of documentation. The "toolbelt" gives them all the access they need to move laterally across the network, exploiting domain administrator level credentials that they either steal or create through elevated privileges, but it's not clear how fully automated some of the steps of that process are. Those steps are likely detailed in a how-to document created by the Dharma RaaS operators.

The ease with which Dharma attackers are able to take these tools and effectively spread ransomware on victims' networks demonstrates the risks posed by both grey hat and legitimate but potentially unwanted administrative tools. And it underlines the risks associated with improperly secured RDP servers, the major vector for most targeted ransomware attacks. Given that many of these attacks are made with stolen credentials purchased in forums, the Dharma attacks may be just one of many intrusions onto victims' networks.

The majority of these Dharma affiliate attacks can be blunted by ensuring RDP servers are patched and secured behind a VPN with multi-factor authentication. Organizations need to remain vigilant about credential theft through phishing, particularly as they adjust to having more employees working remotely. And attention needs to be paid to access given to to service providers and other third parties for business purposes.

Sophos detects the tools mentioned in this report as malware or PUAs. And data collected by Sophos MTR helps continuously improve detections of Dharma attacks. A full list of indicators of compromise, including detection names for the tools and malware mentioned in this report, can be found on SophosLabs' GitHub page here.

SophosLabs would like to acknowledge the contributions of Anand Ajjan, Andrew O'Donnell and Gabor Szappanos of SophosLabs, and Syed Shahram Ahmed and Peter Mackenzie of the Sophos MTR Incident Response team to this report.