

## Attackers linger on government agency computers before deploying Lockbit ransomware

Threat actors spent more than five months remotely googling for tools from the target's machines Written by [Andrew Brandt](#), [Angela Gunn](#) [April 12, 2022](#) [Security Operations](#) [Threat Research](#) [AnyDesk](#) [featured](#) [LockBit Ransomware](#) [Mega](#) [mimikatz](#) [Ransomware](#) [RDP Brute Forcer](#) [RDP Multi Tool](#) [ScreenConnect](#)

In an attack where unknown threat actor groups spent at least five months poking around inside the network of a regional US government agency, behavioral log data suggests that two or more such groups were active before the final group deployed a Lockbit ransomware payload earlier this year.

Throughout the period attackers were active on the target's network, they installed, then used Chrome browser to search for (and download) hacking tools on the "patient zero" computer, a server, where they made their initial access. Though the attackers deleted many Event Logs from machines they controlled, they didn't remove them all.

Name/C2/File/Path/Key/Task/DecodedCommand..etc
hXXps://www.google[.]com/search?q=rdpguard&oq=rdpguard&aqs=chrome..69i57j0i512l9.2322j0j4&sourceid=chrome&ie=UTF-8
hXXps://www.google[.]com/search?q=rdpguard&oq=rdpguard&aqs=chrome..69i57j0i512l9.2322j0j4&sourceid=chrome&ie=UTF-8
hXXps://rdpguard[.]com/download.aspx
hXXps://myip.ms/
hXXps://www.google[.]com/search?q=cryptotab+browser&rlz=1C1CHBD_enUS978US978&oq=cryptotab+browser&aqs=chrome..69i57j0i512l9.6995j0j7&sourceid=chrome&ie=UTF-8
hXXps://www.google[.]com/search?q=cryptotab+browser&rlz=1C1CHBD_enUS978US978&oq=cryptotab+browser&aqs=chrome..69i57j0i512l9.6995j0j7&sourceid=chrome&ie=UTF-8
hXXps://cryptobrowser.site/
hXXps://cryptobrowser.site/en/

Reconstructed from logs, analysts found evidence the threat actors searched for (then downloaded) tools using a Chrome browser they installed on the compromised server

Sophos was able to piece together the narrative of the attack from those unmolested logs, which provide an intimate look into the actions of a not particularly sophisticated, but still successful, attacker.

For instance, the logs recorded that the attackers installed various commercial remote-access tools on accessible servers and desktops. They appeared to prefer the IT management tool ScreenConnect, but later switched to AnyDesk in an attempt to evade our countermeasures. We also found download logs of various RDP scanning, exploit, and brute-force password tools, and records of successful uses of those tools, so Windows remote desktop was on the menu, too.

In addition to various custom scripts and configuration files used by hacking tools the attackers installed, we found a wide variety of other malicious software, from password brute-forcers, to cryptominers, to pirated versions of commercial VPN client software. There was also evidence the attackers used freeware tools like PsExec, FileZilla, Process Explorer, or GMER to execute commands, move data from one machine to another, and kill or subvert the processes that impeded their efforts.

Name/C2/File/Path/Key/Task/DecodedCommand..etc	Description
C:\Windows\System32\cmd.exe	'Discovery_2b (T1018)' malicious behavior detected in 'C:\Windows\System32\cmd.exe'
C:\Windows\System32\cmd.exe	'Discovery_2b (T1018)' malicious behavior detected in 'C:\Windows\System32\cmd.exe'
C:\Windows\System32\cmd.exe	'Discovery_2b (T1018)' malicious behavior detected in 'C:\Windows\System32\cmd.exe'
C:\Windows\System32\cmd.exe	'Discovery_2b (T1018)' malicious behavior detected in 'C:\Windows\System32\cmd.exe'
██████████\Downloads\TemplatesSetup.exe	PUA detected: 'Generic ML PUA' at ██████████\Downloads\TemplatesSetup.exe'
C:\Users\Administrator\AppData\Local\Temp\15\is-3926V.tmp\IObitUnlocker.dll	PUA detected: 'IObit Unlocker' at 'C:\Users\Administrator\AppData\Local\Temp\15\is-3926V.tmp\IObitUnlocker.dll'
C:\Users\Administrator\AppData\Local\Temp\15\uvs\wopesb	PUA detected: 'Universal Virus Sniffer' at 'C:\Users\Administrator\AppData\Local\Temp\15\uvs\wopesb'
C:\Program Files\Process Hacker\x86\ProcessHacker.exe	PUA detected: 'Generic ML PUA' at 'C:\Program Files\Process Hacker\x86\ProcessHacker.exe'
C:\Program Files\Process Hacker\kprocesshacker.sys	PUA detected: 'Process Hacker' at 'C:\Program Files\Process Hacker\kprocesshacker.sys'
C:\Users\Administrator\AppData\Local\Temp\15>PasswordFiles\gmer.exe	PUA detected: 'GMER' at 'C:\Users\Administrator\AppData\Local\Temp\15>PasswordFiles\gmer.exe'

Evidence left behind show the attackers using tools like GMER, IObit Unlocker, and Process Hacker to try to disable endpoint protection

Critically, technicians managing the target network left a protective feature disabled after they completed maintenance. As a result, some systems were left vulnerable to sabotage by attackers, who disabled endpoint protection on the servers and some desktops. With no protection in place, the attackers installed ScreenConnect to give themselves a backup method of remote access, then moved quickly to exfiltrate files from file servers on the network to cloud storage provider Mega.

Name/C2/File/Path/Key/Task/DecodedCommand..etc
mstsc /v: [REDACTED]
7045 - A new service was installed in the system
"C:\Users\admin\Documents\putty.exe"
"C:\Users\admin\Documents\putty.exe"
"C:\Users\admin\Documents\putty.exe"
"C:\Users\admin\Documents\putty.exe"
7045 - A new service was installed in the system
A service was installed in the system.
Service Name: ScreenConnect Client (9d0bbd19cd578d22)
Service File Name: "C:\Program Files (x86)\ScreenConnect Client (9d0bbd19cd578d22)\ScreenConnect.ClientService.exe"
"?e=Access&y=Guest&h=[REDACTED]&p=443&s=[REDACTED]-be56e99c66d6&k=BgIAAACKAABSU0ExAAgAAAEAAQCRIEKbT8x6O770ZKG7xS3kx1A1wNoR
[REDACTED]
5eB4vmDE0AVEEtxEDVVuUmz0rv4t7dhv7IAjQ%2bv7eLA&t=&c=test&c=&c=&c=&c=&c=&c=&c="

The Lockbit attacker used multiple internal RDP connections and the Windows SSH client PuTTY, and installed ScreenConnect, in short order

Over time, we found that the attackers’ tactics changed, in some cases so drastically it seemed as though an attacker with very different skills had joined the fray. The nature of the activity recovered from logs and browser history files on the compromised server gave us the impression that the threat actors who first broke in to the network weren’t experts, but novices, and that they may later have transferred control of their remote access to one or more different, more sophisticated groups who, eventually, delivered the ransomware payload.

Reconstructing the attack from logs

Attackers will often delete log data to obfuscate their tracks, and this incident was no exception — the attackers manually deleted nearly all log data about a month prior to investigator discovery. However, a deeper forensic dig indicates that the initial compromise occurred nearly half a year before investigators opened their case. The method of ingress was nothing spectacular — open RDP ports on a firewall that was configured to provide public access to a server.

For a while, it was a relatively quiet invasion. The attackers got a lucky break when the account they used to break in over RDP was not only a local admin on the server, but also had Domain Administrator permissions, which gave it the ability to create admin-level accounts on other servers and desktops.

Reconstructed through searches of browser and application history logs that remained untouched, Sophos analysts were able to build a picture of a network ill-equipped to resist this type of attack, and attackers who seemed to have done little preparation for what to do beyond gaining initial access.

In the course of performing the post-attack analysis, Sophos analysts determined that the attackers used the servers they controlled inside the target’s network to perform Google searches for a variety of hacking tools.

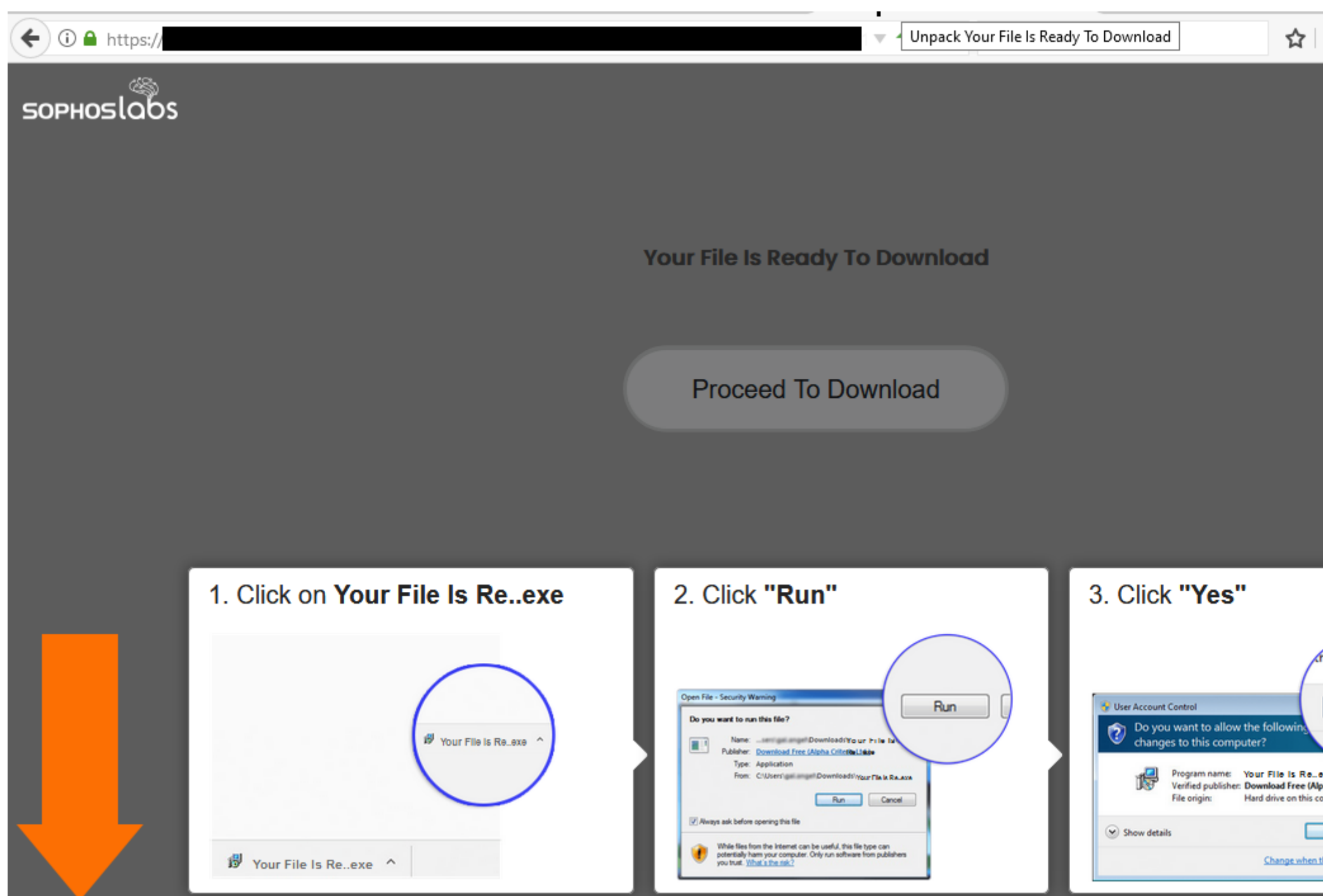


Name/C2/File/Path/Key/Task/DecodedCommand..etc
hXXps://hanner-blobal[.]com/04fc8c09-f8b7-4278-b3ba-3c854aed62c5?siteid=714498&conversion=6496417596617150107
hXXps://aapu.xyz/lp/continue/indextwo.html
hXXps://rinryesop.one/?cs=MzZXNG4CAWEHWAEGZAdcAwNkDF8&abt=0&red=1&sm=16&k=zippyshare%20multi%20tool&v=1.34.23.7&sts=0&prn=0&emb=0&tid=763913&inc=8&u=2217175325704686&fs=1&ref=hXXps%3A%2F%2Fwww111.zippyshare[.]com%2Fv%2FC5LDorfZ%2Ffile.html&osr=ouo[.]io&dstl=hXXps%3A%2F%2Fwww111.zippyshare[.]com%2Fd%2FC5LDorfZ%2F23154%2FRDP_Multi_Tool.rar&jst=0&enr=0&lcua=mozilla%2F5.0%20(windows%20nt%206.3%3B%20win64%3B%20x64)%20applewebkit%2F537.36%20(khtml%2C%20like%20gecko)%20chrome%2F96.0.4664.45%20safari%2F537.36&tzd=-5&uloc=&if=0&ct=1&ctc=4&_Fv6v=1638250162602
hXXps://www.bidderads.xyz/get/campaign/wpcampaign12?postbackid=7004306172371163983&internalid=763913&fname=
hXXps://www.betterex.xyz/ilp/gr/Download-Me.html?partid=wpquicksdf&postbackid=7004306172371163983&internalid=763913&fname=&tk=mtyZodi1mdq0mtm3na%3D%3D
hXXps://rinryesop.one/?cs=S0c0WXN5fgZrR3p0BGhGen8MYUQ&abt=0&red=1&sm=16&k=zippyshare%20multi%20tool&v=1.34.23.7&sts=0&prn=0&emb=0&tid=763913&inc=8&u=2217175325704686&fs=1&ref=hXXps%3A%2F%2Fwww111.zippyshare[.]com%2Fv%2FC5LDorfZ%2Ffile.html&osr=ouo[.]io&dstl=hXXps%3A%2F%2Fwww111.zippyshare[.]com%2Fd%2FC5LDorfZ%2F23154%2FRDP_Multi_Tool.rar&jst=0&enr=0&lcua=mozilla%2F5.0%20(windows%20nt%206.3%3B%20win64%3B%20x64)%20applewebkit%2F537.36%20(khtml%2C%20like%20gecko)%20chrome%2F96.0.4664.45%20safari%2F537.36&tzd=-5&uloc=&if=0&ct=1&ctc=4&_yBD7=1638250191201



Reconstructed browsing logs show the threat actor tried to get RDP Multi Tool from a shady download site, but was beset by aggressive popup ads

In some cases, following the search results for these tools led the attackers into a variety of shady download sites. The advertising networks whose banner ads appear on these sites appear to have generated popup ads that delivered a potentially unwanted app download as the attackers clumsily pulled together a selection of attack tools, further muddying the picture and leaving the server infected with adware, and the browser history cluttered with redirects.



An example of the bogus “download pages” that delivered a potentially unwanted app to the machine the attacker controlled while they tried to download hacking tools

The forensic traces left behind seem to paint a picture of a novice attacker doing a bit of on-the-job training — attempting tool installation (after Googling the tools), opening random text files, and running a surprising number of speed tests, but not moving toward a particular goal or operating with great urgency.

Surviving log data indicates the attacker would leave the server unbothered for days at a time, unexpectedly (and counterintuitively) during American holiday periods. When they were on the system, the attacker seemed to rely on a lot of the shady variety of public file-sharing services, whose advertisements mimic file download links or buttons in an attempt to entice visitors to click their ad instead of the real download button on the page — an ad that typically redirects the visitor into a rotating pool of sites pushing junkware.

Some of the evidence shows the attacker either inadvertently clicked one of these fake-download-button ads, or suffered from popup or popunder advertisements that pushed unwanted downloads at the attacker, who then installed the adware, perhaps thinking it was the real pirated copy of a hack tool they thought they were downloading. These unintentional self-infections created additional noise in the logs.

Unlike many threat actors who pre-configure attack scripts that, for instance, scan networks to determine a target list and then run those scripts to deliver payloads to internal machines, the attackers for months seemed content merely to poke around and occasionally create a new account on the initial, or another, machine. Some of the attacks originated from the Desktop folder of the user account the attackers initially compromised, but others involved admin-level accounts the attackers created with names like ASP.NET or SQL.NET.

Pivot to a more serious attack

In the fifth month of the infiltration, however, the attacker behavior dramatically changed. After a three-week hiatus, logs indicate that an attacker remotely connected and installed the password-sniffing tool Mimikatz. Sophos protections saw it happen, and cleaned a first attempt at infection. Unfortunately, the IT department didn’t heed the warning, and the attacker’s later attempt to run Mimikatz via a compromised account was successful. (The attackers also attempted to gather credentials using a different tool called LaZagne.)

Name/C2/File/Path/Key/Task/DecodedCommand..etc
Visited: Administrator@file:///C:/Users/Administrator/Desktop/mimikatz_trunk/x64/launch.vbs
Visited: Administrator@file:///C:/Users/Administrator/Desktop/mimikatz_trunk/Win32/launch.vbs
C:\Users\Administrator\Desktop\mimikatz_trunk\Win32\mimidrv.sys
C:\Users\Administrator\Desktop\mimikatz_trunk\Win32\mimikatz.exe
C:\Users\Administrator\Desktop\mimikatz_trunk\Win32\mimispool.dll
C:\Users\Administrator\Desktop\mimikatz_trunk\Win32\mimilove.exe
C:\Users\Administrator\Desktop\mimikatz_trunk\Win32\mimilib.dll
C:\Users\Administrator\Desktop\mimikatz_trunk\x64\mimidrv.sys
SOPHOSLABS

Evidence shows the attackers ran Mimikatz on the “Patient Zero” machine’s Administrator account desktop

The credential-dumping application did its work, and within a couple of days, the attackers had a password.txt file sitting on the desktop of the admin-level accounts they’d created on the compromised server. This marks a turning point of sorts in the investigation; at this point, one must assume that any account that had logged into the troubled server was indeed compromised, credentials exposed.

And something else happened: On the same day the passwords.txt file appeared, someone decided to do a bit of tidying up. The initial threat actor, or a newer threat actor, visited websites looking for instructions to uninstall a malicious coinminer that, earlier, had been installed on the beleaguered server.

Scouring log data is a conventional move for an attacker, even one with less dwell time than the attacker in this case. Wiping logs eliminates useful forensic information about the intrusion. The attacker used a compromised account to clear the WitnessClientAdmin, Windows PowerShell, and System logs. By the end of the attack, no event logs prior to about five weeks before the end would be available on the system.

The attacker also spotted the Sophos endpoint installation and tried (unsuccessfully) to remove those as well, using a variety of tools like GMER and IOBit Uninstaller. Via yet another compromised account, the attacker(s) installed an assortment of popular brute-force and proxy tools including NLBrute.

A partial list of maliciously used tools discovered on the compromised system includes the following. It should be noted that not all of these are inherently malicious tools, nor are they all surprising to find on healthy, uninfected machine.

Advanced Port Scanner	Scans to find network devices
AnyDesk	Remote desktop application
LaZagne	Allows users to view and save authentication credentials
Mimikatz	Allows users to view and save authentication credentials
Process Hacker	Multipurpose tool for monitoring system resources
Putty	Terminal emulator, serial console, network file transfers
Remote Desktop Passview	Reveals passwords stored in an .rdp file by Microsoft’s RDP utility
ScreenConnect	Remote desktop application
SniffPass	Password monitoring tool; listens on the network adapter
WinSCP	SFTP/FTP client for copying files between local and remote machines

Suddenly — over four months after the initial compromise — not only are the behaviors of the attackers suddenly crisper, more focused, but the locations of the malicious visitor(s) have expanded, with IP-address traces indicating connections from both Estonia and Iran. Ultimately the compromised network would host malicious visitors from IP addresses that geolocate to Iran, Russia, Bulgaria, Poland, Estonia, and... Canada. But these IP addresses may have been Tor exit nodes.

Ironically, right around this time, the target’s IT department noticed that the systems were “acting strange” — repeatedly rebooting, possibly by the threat actor’s direct command shortly after destroying the event logs. The IT department began its own investigation and would ultimately take five dozen servers offline while they built network segmentation designed to protect known-good devices from the others. However, to cut down on distractions, the IT department disabled Sophos Tamper Protection.


Things got frenetic after that. The last ten days of the infection were full of moves and countermoves made by the attackers and the IT department. On the eighth day, Sophos’ team entered the fray. Through the end of the last calendar month of the attack, a steady stream of table-setting activities took place as the attackers dumped account credentials, ran network enumeration tools, checked their RDP abilities, and created new user accounts, presumably to give themselves options in case they were interrupted in subsequent attacks. The logs were wiped multiple times and machines restarted during this period.

```
All your files have been encrypted!
All your files have been encrypted due to a security problem with your PC. If you want to
restore them, please send an email to rdprecovery@mail.ee
The subject of your email should be: XXXXXXXX
if you didn't get any response you can send an email to XXXxxxxxxxxx@tutanota.com
You have to pay for decryption in Bitcoin. The price depends on how fast you contact us.
After payment we will send you the decryption tool.

- How can you trust us to decrypt your files?
  Before paying you can send us up to 3 files for free decryption. The total size of
  files must be less than 2Mb (non archived), and files should not contain valuable
  information. (databases, backups, large excel sheets, etc.)

- How to obtain Bitcoins
  The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click
  'Buy bitcoins', and select the seller by payment method and price.
  https://localbitcoins.com/buy_bitcoins
  Also you can find other places to buy Bitcoins and beginners guide here:
  http://www.coindesk.com/information/how-can-i-buy-bitcoins/

- Attention!
  Do not rename encrypted files.
  Do not try to decrypt your data using third party software, it may cause permanent
  data loss.
  Decryption of your files with the help of third parties may cause increased price
  (they add their fee to our) or you can become a victim of a scam.
```



One of two ransom notes, found on systems where the files had been renamed with a new file suffix, but not encrypted. Reverting to the original suffix restored access to the files.

On the first day of the sixth month of the attack, the attacker made their big move, running Advanced IP Scanner and almost immediately beginning lateral movement to multiple sensitive servers. Sophos protections knocked down several new attempts at malicious file installation, but compromised credentials allowed the attacker to outflank those protections.

Within minutes, the attacker(s) had access to a slew of sensitive personnel and purchasing files, and attackers were hard at work doing another credential dump.



```
~~~ LockBit 2.0 the fastest ransomware in the world ~~~

>>>> Your data are stolen and encrypted
The data will be published on TOR website if you do not pay the ransom
http://lockbitsapyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy.onion
and https://xxxxxxxxxx.uz (the link for any other browser).

>>>> What guarantees that we will not deceive you?

We are not a politically motivated group and we do not need anything other than your
money.


If you pay, we will provide you the programs for decryption and we will delete your
data.
Life is too short to be sad. Be not sad, money, it is only paper.

If we do not give you decrypters, or we do not delete your data after payment, then
nobody will pay us in the future.
Therefore to us our reputation is very important. We attack the companies worldwide and
there is no dissatisfied victim after payment.

You can obtain information about us on twitter
https://twitter.com/hashtag/lockbit?f=live

>>>> You need contact us and decrypt one file for free on these TOR sites with your personal
decryption ID XXXXXXXXXXXXXXXX

Download and install TOR Browser https://www.torproject.org/
```



The second ransom note, found on machines successfully encrypted with LockBit

The next day, the target engaged with Sophos. Labs analysts identified the 91.191.209.198:4444 as a phone-home address with related shellcode, now detected as ATK/Tlaboc-A and ATK/Shellcode-A. Over the course of several days, the IT team and Sophos analysts collected evidence then quickly shut down servers that provided the attackers with remote access, and worked to remove the malware from the machines that had not been encrypted.

Fortunately for the target, on at least a few machines, the attackers didn't complete their mission, as we found files that had been renamed with a ransomware-related file suffix, but that had not been encrypted. Cleanup in those cases just involved renaming the files to restore their previous file suffixes.

## Guidance and detection

In the course of the investigation, one factor seemed to stand out: The target's IT team made a series of strategic choices that enabled the attackers to move freely and to access internal resources without impediment. Deployment of MFA would have hindered the access by the threat actors, as would a firewall rule blocking remote access to RDP ports in the absence of a VPN connection.

Responding to alerts, or even warnings about reduced performance, promptly would have prevented a number of attack stages from bearing fruit. Disabling features like tamper protection on endpoint security software seemed to be the critical lever the attackers needed to completely remove protection and complete their jobs without hindrance.

The ransomware threat actors added a help wanted ad into their ransom note. Our recommendation is that insiders with access to sensitive information refrain from committing crimes by helping ransomware threat actors.



```
>>>> Advertisement

Would you like to earn millions of dollars $$$ ?

Our company acquire access to networks of various companies, as well as insider
information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and
password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your
company.

You can do it both using your work computer or the computer of any other employee in
order to divert suspicion of being in collusion with us.

Companies pay us the foreclosure for the decryption of files and prevention of data
leak.

You can contact us using Tox messenger without registration and SMS
https://tox.chat/download.html.
Using Tox messenger, we will never know your real name, it means your privacy is
guaranteed.

If you want to contact us, use Tox ID
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

If this contact is expired, and we do not respond you, look for the relevant contact
data on our website via Tor or Brave browser
http://lockbitsapyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy.onion and
https://xxxxxxxxxx.uz (the link for any other browser).
```

SOPHOSLABS

The ransomware binaries deployed in this attack are detected using CryptoGuard and the various dual-purpose attack tools used in the attack are detected as follows. Not all files are routinely detected as many of these utilities have a legitimate IT administrative purpose.

Utility	SHA-256 hash(es)	Sophos definition
Advanced Port Scanner	6684e1df360db67719f65bcd39467cc88bbd7bb910636d03071245b622e7cfa3	
	87bf05057f215659cc801750118900145f8a22fa93ac4c6e1bfd81aa98b0a55	
AnyDesk	4a9dde3979c2343c024c6eeeddf7639be301826dd637c006074e04a1e4e9fe7	
	db385ea6858db4b4cb49897df9ec6d5cc4675aaf675e692466b3b50218e0eeca	
Mimikatz	3d0e06086768500a2bf680ffbed0409d24b355887169b821d55233529ad2c62a	ATK/Mimikatz-AE ATK/Mimikatz-BE
	0d31a6d35d6b320f815c6ba327ccb8946d4d7f771e0dcdbf5aa8af775576f2d1	
NLBrute	83d7f6eaf7fe075503ea6a0bc726633c34595a6eae7edd7deab95ab4d4a66fd5	Mal/Generic-R + Mal/VMProtBad-A
Process Hacker	46367bfcf4b150da573a74d91aa2f7caf7a0789741bc65878a028e91ffbf5e42	
ScreenConnect	89904c4d3b1ebbfd294b1a87940400a2db2ead01b3d6e3e2e151481faae95bd	
	ffbb5241ed488b98725013185c80f40156d32884a87d6898d53e2aef28f1c3f8	

All other shareable IOCs relating to this attack are shown above. Sophos only shares indicators and samples which cannot be tied to a specific target to protect the target’s privacy.

Acknowledgments

SophosLabs would like to acknowledge the contributions of analysts Melissa Kelly, Peter Mackenzie, Ferenc László Nagy , Mauricio Valdivieso, Sergio Bestulic, Johnathan Fern, Linda Smith, and Matthew Everts for their work reconstructing the attack.

- [Share on Facebook](#)
- [Share on Twitter](#)
- [Share on LinkedIn](#)
-