They’re back: inside a new Ryuk ransomware attack

news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/

Sean Gallagher

October 14, 2020

The operators of Ryuk ransomware are at it again. After a long period of quiet, we identified a new spam campaign linked to the Ryuk actors—part of a new wave of attacks. And in late September, Sophos’ Managed Threat Response team assisted an organization in mitigating a Ryuk attack—providing insight into how the Ryuk actors’ tools, techniques and practices have evolved. The attack is part of a recent wave of Ryuk incidents tied to recent phishing campaigns.

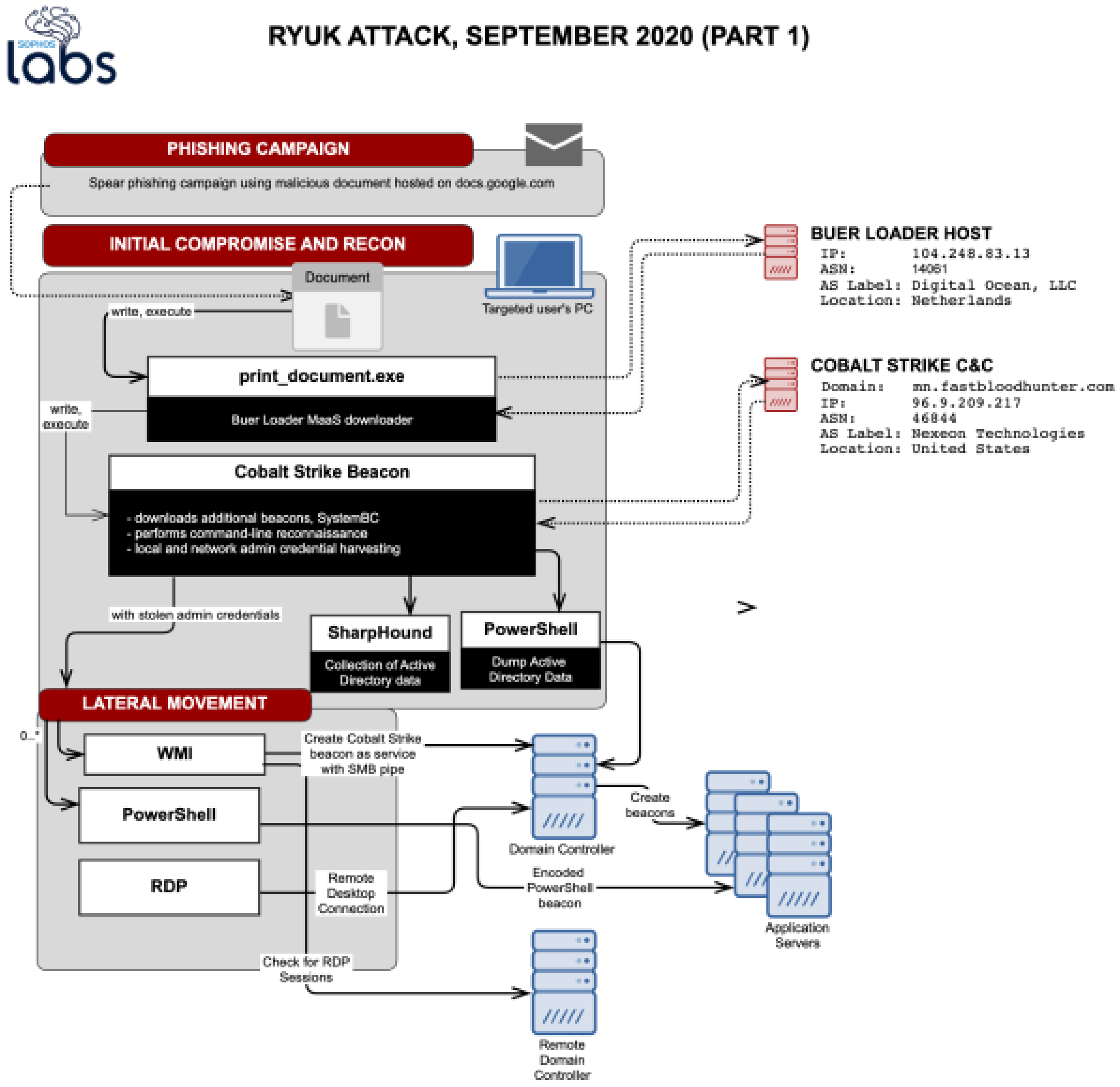
First spotted in August of 2018, the Ryuk gang gained notoriety in 2019, demanding multi-million-dollar ransoms from companies, hospitals, and local governments. In the process, the operators of the ransomware pulled in over $61 million just in the US, according to figures from the Federal Bureau of Investigation. And that’s just what was reported—other estimates place Ryuk’s take in 2019 in the hundreds of millions of dollars.

Starting around the beginning of the worldwide COVID-19 pandemic, we saw a lull in Ryuk activity. There was speculation that the Ryuk actors had moved on to a rebranded version of the ransomware, called Conti. The campaign and attack we investigated was interesting both because it marked the return of Ryuk with some minor modifications, but also showed an evolution of the tools used to compromise targeted networks and deploy the ransomware.

The attack was also notable because of how quickly the attacks can move from initial compromise to ransomware deployment. Within three and a half hours of a target opening a phishing email attachment, attackers were already conducting network reconnaissance. Within a day, they had gained access to a domain controller, and were in the early stages of an attempt to deploy ransomware.

The attackers were persistent as well. As attempts to launch the attack failed, the Ryuk actors attempted multiple times over the next week to install new malware and ransomware, including renewed phishing attempts to re-establish a foothold. Before the attack had concluded, over 90 servers and other systems were involved in the attack, though ransomware was blocked from full execution.

Let the wrong one in


SOPHOS labs
RYUK ATTACK, SEPTEMBER 2020 (PART 1)
PHISHING CAMPAIGN
Spear phishing campaign using malicious document hosted on docs.google.com
INITIAL COMPROMISE AND RECON
Document
Targeted user's PC
write, execute
print_document.exe
Buer Loader MaaS downloader
write, execute
Cobalt Strike Beacon
- downloads additional beacons, SystemBC
- performs command-line reconnaissance
- local and network admin credential harvesting
with stolen admin credentials
SharpHound
Collection of Active Directory data
PowerShell
Dump Active Directory Data
BUER LOADER HOST
IP: 104.248.83.13
ASN: 14061
AS Label: Digital Ocean, LLC
Location: Netherlands
COBALT STRIKE C&C
Domain: mn.fastbloodhunter.com
IP: 96.9.209.217
ASN: 46844
AS Label: Nexeon Technologies
Location: United States
LATERAL MOVEMENT
0..*
WMI
PowerShell
RDP
Create Cobalt Strike beacon as service with SMB pipe
Remote Desktop Connection
Check for RDP Sessions
Domain Controller
Create beacons
Encoded PowerShell beacon
Application Servers
Remote Domain Controller

Initial compromise, reconnaissance and lateral movement phase of Ryuk attack
The attack began on the afternoon of Tuesday. September 22. Multiple employees of the targeted company had received highly-targeted phishing emails:

> From: Alex Collins [spoofed external email address]
>
> To: [targeted individual]
>
> Subject: Re: [target surname] about debit
>
> Please call me back till 2 PM, i will be in [company name] office till 2 PM.
>
> [Target surname], because of [company name]head office **request #96-9/23** [linked to remote file], i will process additional 3,582 from your payroll account.
>
> [Target first name], call me back when you will be available to confirm that all is correct.
>
> Here is a copy of your **statement in PDF**[linked to remote file].
>
> Alex Collins
>
> [Company name] outsource specialist

The link, served up through the mail delivery service Sendgrid, redirected to a malicious document hosted on docs.google.com. The email was tagged with external sender warnings by the company's mail software. And multiple instances of the malicious attachment were detected and blocked.

But one employee clicked on the link in the email that afternoon. The user opened the document and enabled its content, allowing the document to execute **print_document.exe**—a malicious executable identified as Buer Loader. Buer Loader is a modular malware-as-a-service downloader, introduced on underground forums for sale in August of 2019. It provides a web panel-managed malware distribution service; each downloader build sold for $350, with add-on modules and download address target changes billed separately.

In this case, upon execution, the Buer Loader malware dropped **qoipozincyusury.exe**, a Cobalt Strike "beacon," along with other malware files. Cobalt Strike's beacon, originally designed for attacker emulation and penetration testing, is a modular attack tool that can perform a wide range of tasks, providing access to operating system features and establishing a covert command and control channel within the compromised network.

Over the next hour and a half, additional Cobalt Strike beacons were detected on the initially compromised system. The attackers were then able to successfully establish a foothold on the targeted workstation for reconnaissance and to hunt for credentials.

A few hours later, the Ryuk actors' reconnaissance of the network began. The following commands were run on the initially infected system:

- C:\WINDOWS\system32\cmd.exe /C whoami /groups (accessing list of AD groups the local user is in)

- C:\WINDOWS\system32\cmd.exe /C nltest /domain_trusts /all_trusts (returns a list of all trusted domains)
- C:\WINDOWS\system32\cmd.exe /C net group “enterprise admins” /domain (returns a list of members of the “enterprise admins” group for the domain)
- C:\WINDOWS\system32\net1 group “domain admins” /domain (the same, but a list of the group “domain admins”)
- C:\WINDOWS\system32\cmd.exe /C net localgroup administrators (returns a list of administrators for the local machine)
- C:\WINDOWS\system32\cmd.exe /C ipconfig (returns the network configuration)
- C:\WINDOWS\system32\cmd.exe /C nltest /dclist:[target company domain name] (returns names of the domain controllers for the company domain name)
- C:\WINDOWS\system32\cmd.exe /C nltest /dclist:[target company name] (the same, but checking for domain controllers using the company name as the domain name)

Forward lateral

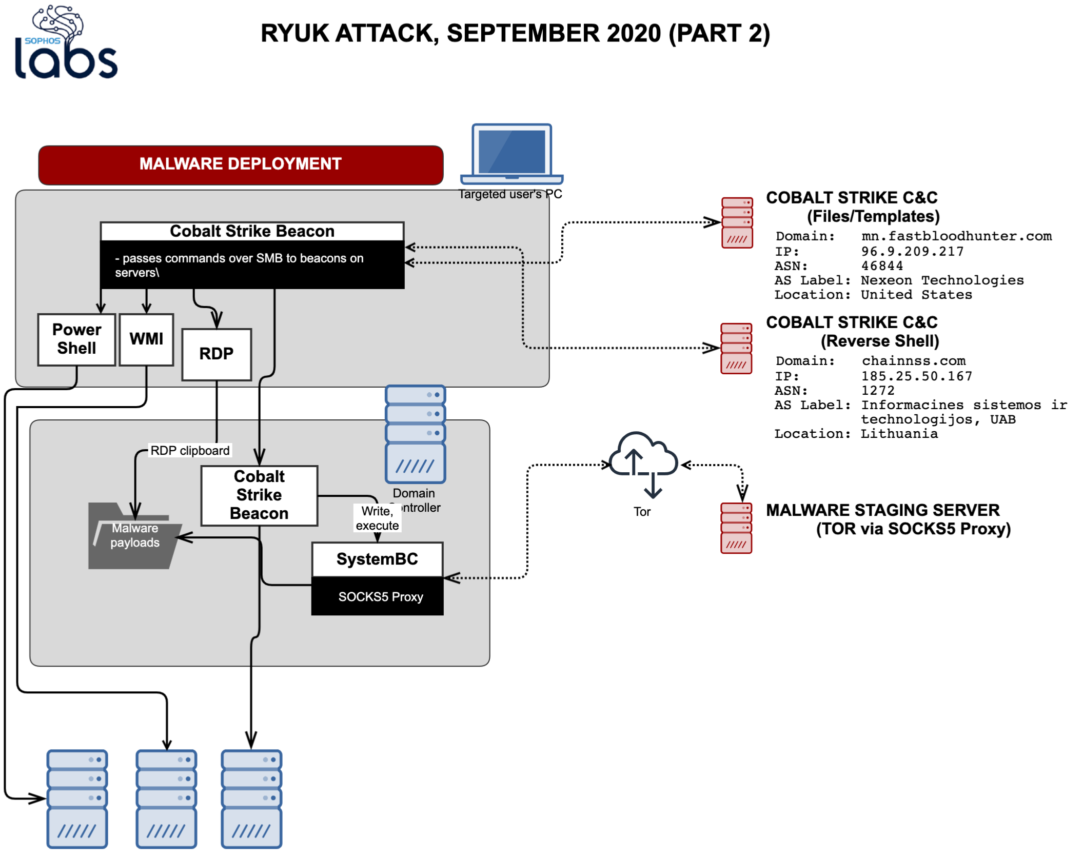
Using this data, by Wednesday morning the actors had obtained administrative credentials and had connected to a domain controller, where they performed a data dump of Active Directory details. This was most likely accomplished through the use of **SharpHound**, a Microsoft C#-based data “injestor” tool for BloodHound (an open-source Active Directory analysis tool used to identify attack paths in AD environments). A data dump from the tool was written to a user directory for the compromised domain administrator account on the domain server itself.

Another Cobalt Strike executable was loaded and launched a few hours later. That was followed immediately by the installation of a Cobalt Strike service on the domain controller using the domain administrator credentials obtained earlier. The service was a chained Server Message Block listener, allowing Cobalt Strike commands to be passed to the server and other computers on the network. Using Windows Management Interface, the attackers remotely executed a new Cobalt Strike beacon on the same server.

In short order, other malicious services were created on two other servers using the same admin credentials, using Windows Management Instrumentation from the initially compromised PC. One of the services configured was an encoded PowerShell command creating yet another Cobalt communications pipe.

The actors continued to perform reconnaissance activities from the initially infected desktop, executing commands trying to identify potential targets for further lateral movement. Many of these repeated previous commands. The **nltest** command was used in an attempt to retrieve data from domain controllers on other domains within the enterprise Active Directory tree. Other commands pinged specific servers, attempting to gain IP addresses. The actors also checked against all mapped network shares connected to the workstation and used WMI to check for active Remote Desktop sessions on another domain controller within the Active Directory tree.

Setting the trap



Late Wednesday afternoon—less than a day after the victim's click on the phish— the Ryuk actors began preparations to launch their ransomware. Using the beachhead on the initially compromised PC, the attackers used RDP to connect to the domain controller with the admin credentials obtained the day before. A folder named **C:\Perflogs\grub.info.test2 – Copy** was dropped on the domain controller— a name consistent with a set of tools deployed in previous Ryuk attacks. A few hours later, the attackers ran an encoded PowerShell command that, accessing Active Directory data, generated a dump file called **ALLWindows.csv**, containing login, domain controller and operating system data for Windows computers on the network.

Next, the **SystemBC** malicious proxy was deployed on the domain controller. SystemBC is a SOCKS5 proxy used to conceal malware traffic that shares code and forensic markers with other malware from the Trickbot family. The malware installed itself (as itvs.exe), and created a scheduled job for the malware, using the old Windows task scheduler format in a file named itvs.job—in order to maintain persistence.

A PowerShell script loaded into the **grub.info.test** folder on the domain controller was executed next. This script, **Get.DataInfo.ps1** , scans the network and provides an output of which systems are active. It also checks which AV is running on the system.

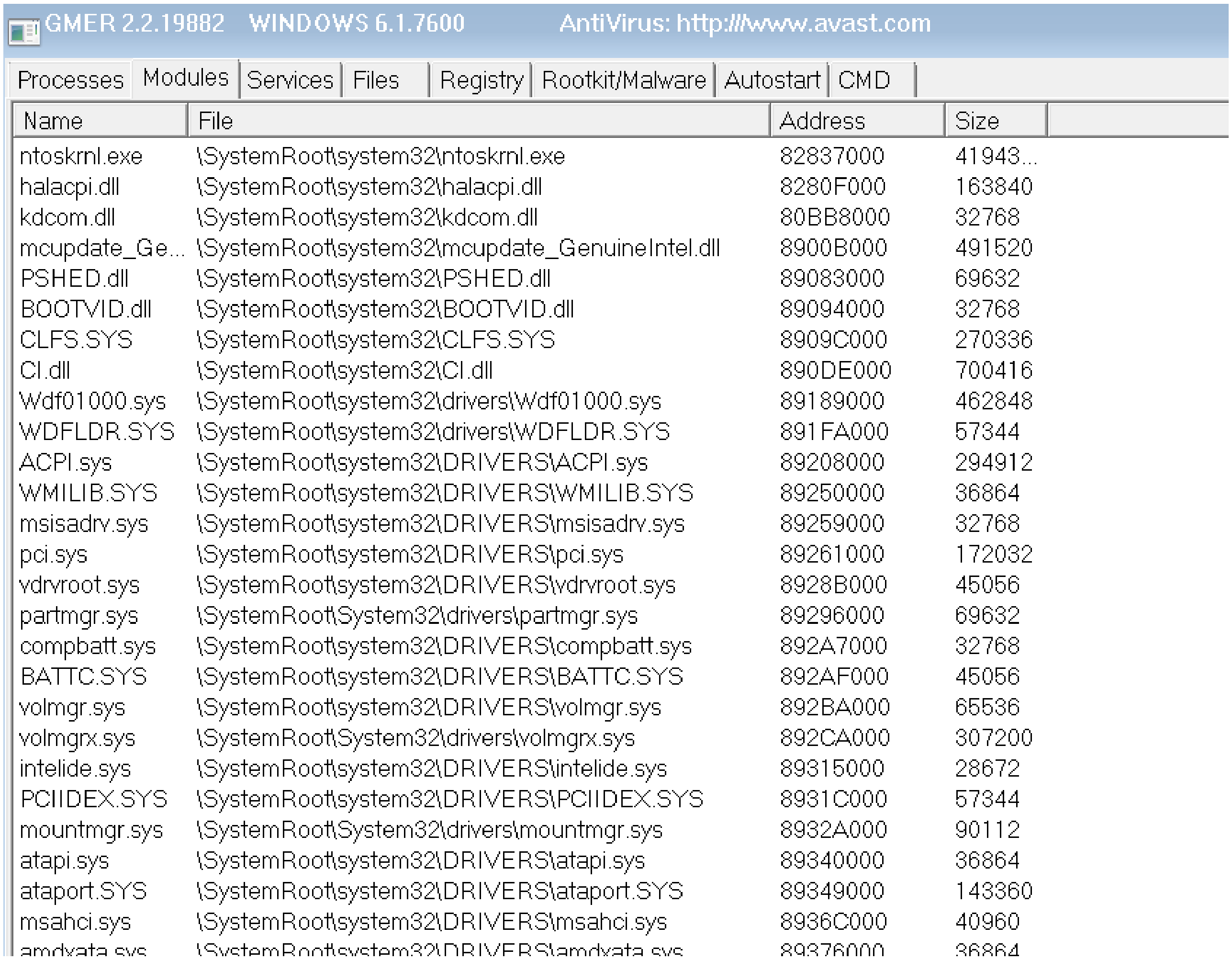
The Ryuk actors used a number of methods to attempt to spread files to additional servers, including file shares, WMI, and Remote Desktop Protocol clipboard transfer. WMI was used to attempt to execute GetDataInfo.ps1 against yet another server.

Failure to launch

Thursday morning, the attackers spread and launched Ryuk. This version of Ryuk had no substantial changes from earlier versions we've seen in terms of core functionality, but Ryuk's developers did add more obfuscation to the code to evade memory-based detections of the malware.

The organizational backup server was among the first targeted. When Ryuk was detected and stopped on the backup server, the attackers used the icacls command to modify access control, giving them full control of all the system folders on the server.

They then deployed **GMER**, a "rootkit detector" tool:



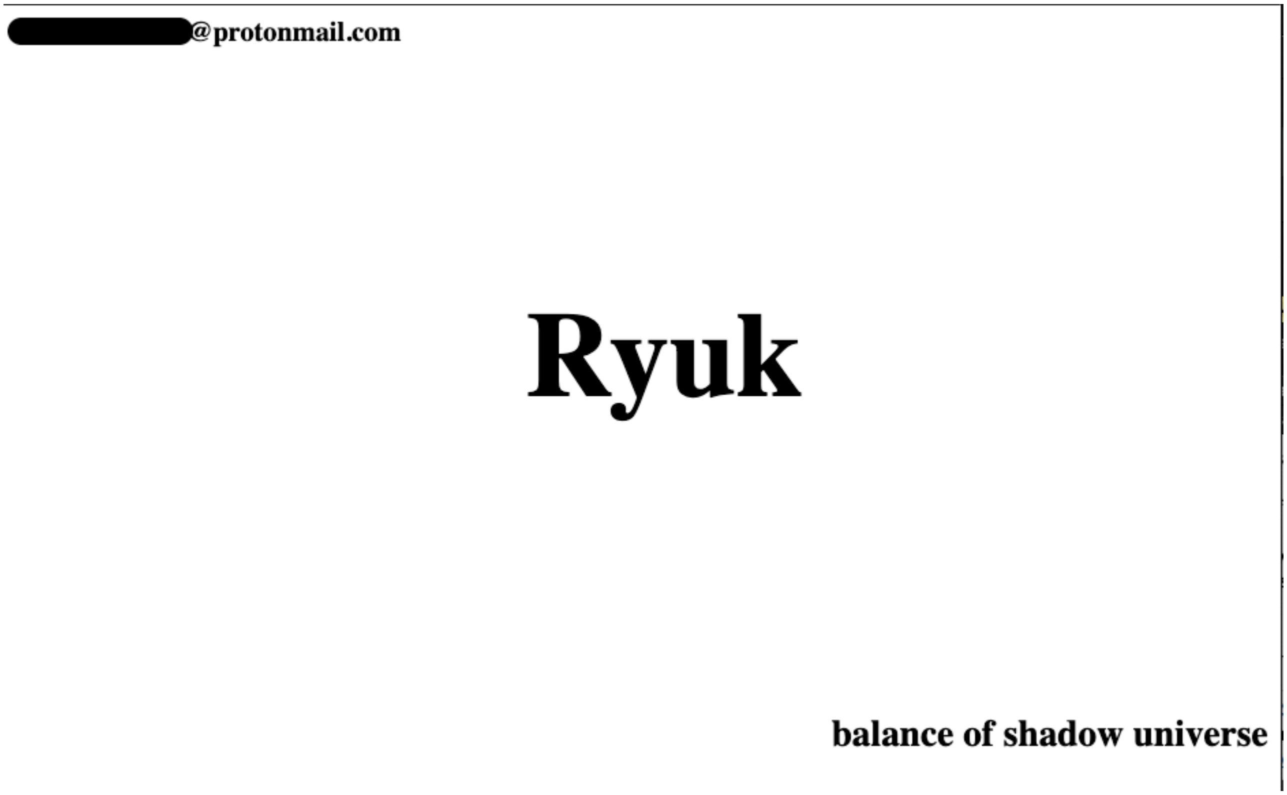
GMER 2.2.19882   WINDOWS 6.1.7600   AntiVirus: http://www.avast.com
Processes
Modules
Services
Files
Registry
Rootkit/Malware
Autostart
CMD

Name	File	Address	Size
ntoskrnl.exe	\SystemRoot\system32\ntoskrnl.exe	82837000	41943...
halacpi.dll	\SystemRoot\system32\halacpi.dll	8280F000	163840
kdcom.dll	\SystemRoot\system32\kdcom.dll	80BB8000	32768
mcupdate_Ge...	\SystemRoot\system32\mcupdate_GenuineIntel.dll	8900B000	491520
PSHED.dll	\SystemRoot\system32\PSHED.dll	89083000	69632
BOOTVID.dll	\SystemRoot\system32\BOOTVID.dll	89094000	32768
CLFS.SYS	\SystemRoot\system32\CLFS.SYS	8909C000	270336
CI.dll	\SystemRoot\system32\CI.dll	890DE000	700416
Wdf01000.sys	\SystemRoot\system32\drivers\Wdf01000.sys	89189000	462848
WDFLDR.SYS	\SystemRoot\system32\drivers\WDFLDR.SYS	891FA000	57344
ACPI.sys	\SystemRoot\system32\DRIVERS\ACPI.sys	89208000	294912
WMILIB.SYS	\SystemRoot\system32\DRIVERS\WMILIB.SYS	89250000	36864
msisadrv.sys	\SystemRoot\system32\DRIVERS\msisadrv.sys	89259000	32768
pci.sys	\SystemRoot\system32\DRIVERS\pci.sys	89261000	172032
vdrvroot.sys	\SystemRoot\system32\DRIVERS\vdrvroot.sys	8928B000	45056
partmgr.sys	\SystemRoot\System32\drivers\partmgr.sys	89296000	69632
compbatt.sys	\SystemRoot\system32\DRIVERS\compbatt.sys	892A7000	32768
BATTC.SYS	\SystemRoot\system32\DRIVERS\BATTC.SYS	892AF000	45056
volmgr.sys	\SystemRoot\system32\DRIVERS\volmgr.sys	892BA000	65536
volmgrx.sys	\SystemRoot\System32\drivers\volmgrx.sys	892CA000	307200
intelide.sys	\SystemRoot\system32\DRIVERS\intelide.sys	89315000	28672
PCIIDEX.SYS	\SystemRoot\system32\DRIVERS\PCIIDEX.SYS	8931C000	57344
mountmgr.sys	\SystemRoot\System32\drivers\mountmgr.sys	8932A000	90112
atapi.sys	\SystemRoot\system32\DRIVERS\atapi.sys	89340000	36864
ataport.SYS	\SystemRoot\system32\DRIVERS\ataport.SYS	89349000	143360
msahci.sys	\SystemRoot\system32\DRIVERS\msahci.sys	8936C000	40960
amdxata.sys	\SystemRoot\system32\DRIVERS\amdxata.sys	89376000	36864

The GMER process hunting tool.

GMER is frequently used by ransomware actors to find and shut down hidden processes, and to shut down antivirus software protecting the server. The Ryuk attackers did this, and then they tried again. Ryuk ransomware was redeployed and re-launched three more times in short order, attempting to overwhelm remaining defenses on the backup server.

Ransom notes were dropped in the folders hosting the ransomware, but no files were encrypted.



[redacted]@protonmail.com

Ryuk

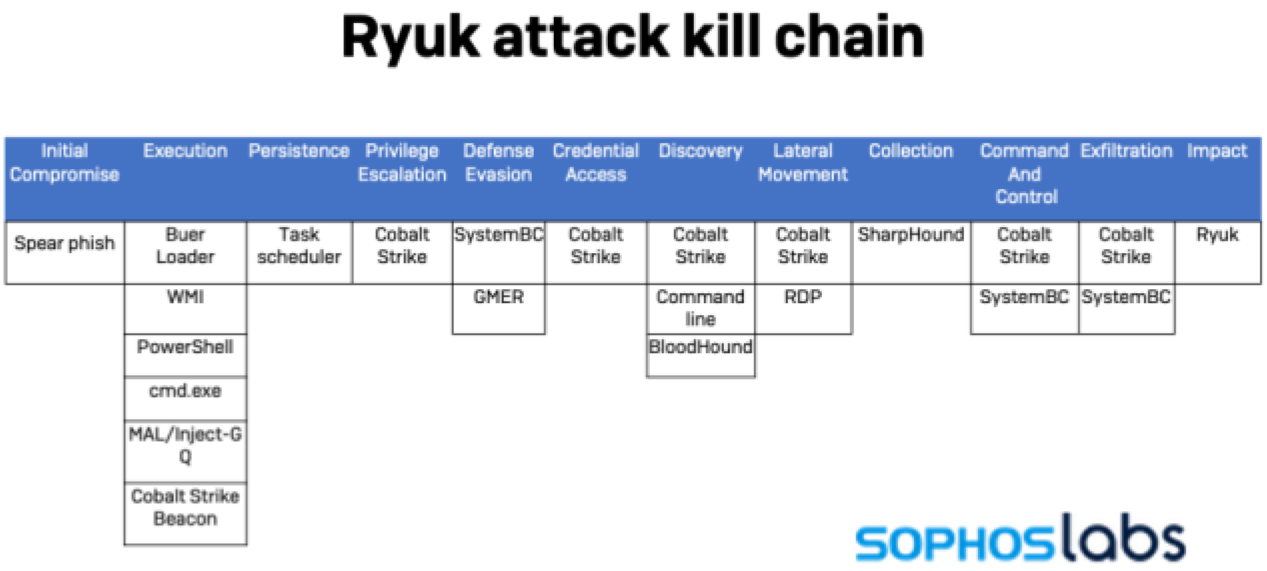
balance of shadow universe

The Ryuk HTML ransom note.

In total, Ryuk was executed in attacks launched from over 40 compromised systems,but was repeatedly blocked by Sophos Intercept X. By noon on Thursday, the ransomware portion of the attack had been thwarted. But the attackers weren’t done trying—and weren’t off the network yet.

On Friday, defenders deployed a block across the domains affected by the attack for the SystemBC RAT. The next day, the attackers attempted to activate another SOCKS proxy on the still-compromised domain controller. And additional Ryuk deployments were detected over the following week—along with additional phishing attempts and attempts to deploy Cobalt Strike.

Lessons learned



Ryuk attack kill chain

Initial Compromise	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Spear phish	Buer Loader	Task scheduler	Cobalt Strike	SystemBC	Cobalt Strike	Cobalt Strike	Cobalt Strike	SharpHound	Cobalt Strike	Cobalt Strike	Ryuk
	WMI			GMER		Command line	RDP		SystemBC	SystemBC	
	PowerShell					BloodHound					
	cmd.exe										
	MAL/Inject-GQ										
	Cobalt Strike Beacon										

sophoslabs

The Ryuk attack's exploitation chain.

The tactics exhibited by the Ryuk actors in this attack demonstrate a solid shift away from the malware that had been the basis of most Ryuk attacks last year (Emotet and Trickbot). The Ryuk gang shifted from one malware-as-a-service provider (Emotet) to another (Buer Loader), and has apparently replaced Trickbot with more hands-on-keyboard exploitation tools—Cobalt Strike, Bloodhound, and GMER, among them—and built-in Windows scripting and administrative tools to move laterally within the network. And the attackers are quick to change tactics as opportunities to exploit local network infrastructure emerge—in another recent attack Sophos responded to this month, the Ryuk actors also used Windows Global Policy Objects deployed from the domain controller to spread ransomware. And other recent attacks have used another Trickbot-connected backdoor known as Bazar.

The variety of tools being used, including off-the-shelf and open-source attack tools, and the volume and speed of attacks is indicative of an evolution in the Ryuk gang's operational skills. Cobalt Strike's "offensive security" suite is a favorite tool of both state-sponsored and criminal actors, because of its relative ease of use and broad functionality, and its wide availability—"cracked" versions of the commercially-licensed software are readily purchased in underground forums. And the software provides actors with a ready-made toolkit for exploitation, lateral movement, and many of the other tasks required to steal data, escalate the compromise and launch ransomware attacks without requiring purpose-made malware.

While this attack happened quickly, the persistence of the attacks following the initial failure of Ryuk to encrypt data demonstrate that the Ryuk actors—like many ransomware attackers—are slow to unlatch their jaws, and can persist for long periods of time once they've moved laterally within the network and can establish additional backdoors. The attack also shows that Remote Desktop Protocol can be dangerous even when it is inside the firewall.

IOCs for this attack are posted on the SophosLabs GitHub here.

SophosLabs would like to acknowledge the contributions of Peter Mackenzie, Elida Leite, Syed Shahram and Bill Kearney of the MTR team, and Anand Aijan, Sivagnanam Gn, and Suraj Mundalik of SophosLabs to this report.