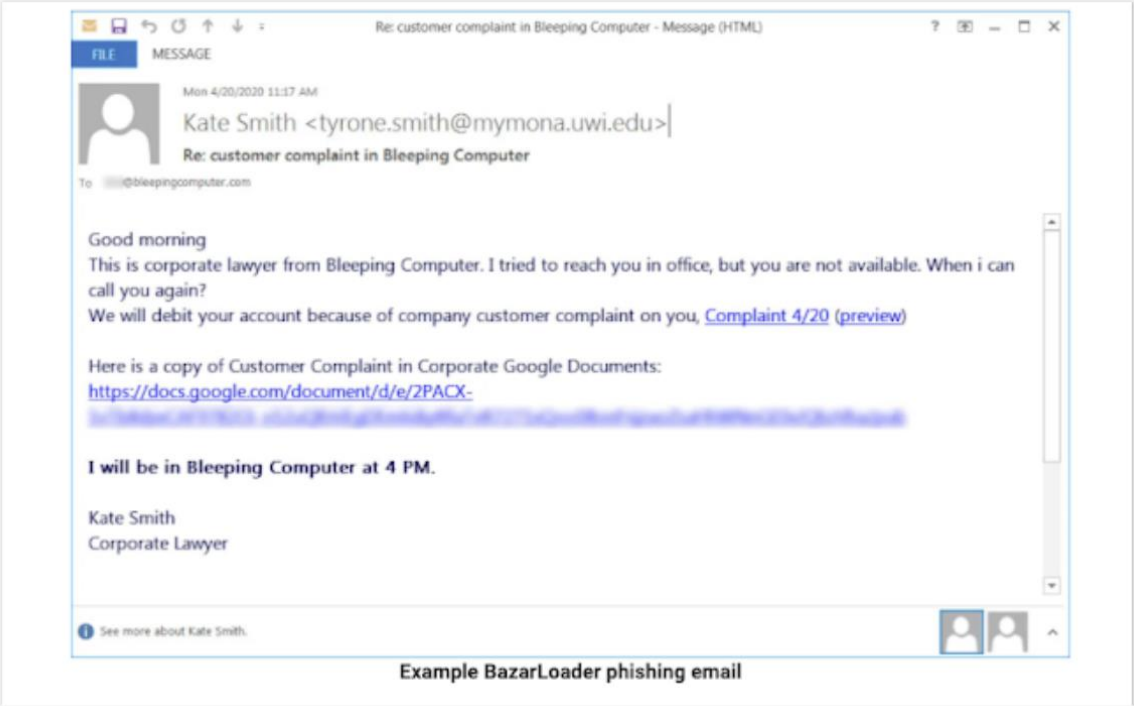
Ryuk

Initial Access

- **Spearphishing**
  - https://www.advintel.io/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon
  - Legitimate and widely used **SendGrid** email marketing platform
  - Decoy google preview page to trick the user into downloading
  - Malicious files are certificate signing to evading anti-virus
  - Downloads encrypted BazarBackdoor



Example BazarLoader phishing email

- **Bazar Execution**
  - https://www.advintel.io/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon
  - **https://attack.mitre.org/software/S0534/**
  - Bazar relies on user execution of an executable to run.
  - This user was a Domain User and did not have any other permissions.
  - Injects malicious code into one of the following processes: cmd, explorer, and svchost
  - Scheduled task with the name such as "StartAd - Ad" is created, the loader writes itself into the Windows registry, and creates autorun entries
  - Download and execute the BazarBackdoor and Cobalt Strike beacons to further access once inside the targeted networks

Privilege Escalation

- **CVE-2020-1472**
  - https://resources.infosecinstitute.com/topic/zerologon-cve-2020-1472-technical-overview-and-walkthrough/
  - Attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol
  - The attack is possible by taking advantage of the incorrect use of an AES mode of operating during the cryptographic process to spoof the identity of any computer account, including the DC itself, and thus setting an empty password for that account locally.
  - In order to exploit this vulnerability, attackers must be able to set up a TCP connection with the DC server from the internal network or even exploiting a webserver online, compromising it and breaking the barriers of a potential DMZ misconfigured (a scenario exploited in the wild by criminals and presented towards the end of the article).

Defense Evasion

- **Signed Binary Proxy Execution: Rundll32**
  - https://attack.mitre.org/techniques/T1218/011/
  - Adversaries may abuse rundll32.exe to proxy execution of malicious code. Using rundll32.exe, vice executing directly (i.e. Shared Modules), may avoid triggering security tools that may not monitor execution of the rundll32.exe process because of allowlists or false positives from normal operations. Rundll32.exe is commonly associated with executing DLL payloads.
  - CVE-2020-14 On the first domain controller that the treat actors connected to after their initial connection, they dropped a DLL and executed it via rundll32.
  - Dropped via RDP and executed via rundll32 on the second domain controller.
  - Shortly after, the DLL was called again via regsrv32.
  - Then a 2nd DLL was dropped and executed in a similar manner on the 2nd DC.

Discovery

- **Active Directory**
  - **https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/**
  - Ran on the beachhead.
    - nltest /domain_trusts /all_trusts
    - nltest /dclist:DOMAIN
    - net group "Domain admins" /DOMAIN
  - Ran on a domain controller.
    - net group "enterprise admins" /domain
    - nltest /domain_trusts /all_trusts
    - nltest /dclist:"DOMAIN"
    - ping DOMAINCONTROLLER
    - cmd.exe /C time
    - net user administrator /domain
  - They then ran the following looking for host names, operating systems and last logon dates of all AD systems.
    - C:\Windows\system32\cmd.exe /C Get-ADComputer -Filter {enabled -eq $true} -properties *|select Name, DNSHostName, OperatingSystem, LastLogonDate | Export-CSV C:\Users\AllWindows.csv -NoTypeInformation -Encoding UTF8
  - After already completing the above discovery work and having already pivoted to their 2nd domain controller, the threat actors moved on to AdFind for further domain reconnaissance.
    - C:\Windows\Temp\adf\AdFind.exe
    - C:\Windows\Temp\adf\adf.bat
  - Contents of the script ran the following with AdFind.
    - adfind.exe -f "(objectcategory=person)"
    - adfind.exe -f "objectcategory=computer"
    - adfind.exe -f "(objectcategory=organizationalUnit)"
    - adfind.exe -sc trustdmp
    - adfind.exe -subnets -f (objectCategory=subnet)
    - adfind.exe -f "(objectcategory=group)"
    - adfind.exe -gcb -sc trustdmp
  - The threat actor then ran this command a few times.
    - nltest /domain_trusts /all_trusts

Lateral Movement

- **Valid Accounts**
  - **https://attack.mitre.org/techniques/T1021/002/**
    - An executable was transferred to it via SMB using a domain administrator account.
  - **https://attack.mitre.org/techniques/T1021/006/**
    - After transferring the exe, the threat actors utilized WMI from the beachhead host to execute the file.
  - The presence of the EICAR strings point to the Cobalt Strike software being used as a trial version.
  - **https://attack.mitre.org/techniques/T1021/001/**
    - Shortly there after we saw a Cobalt Strike DLL transferred via the RDP connection.
    - RDP was used to pivot from the main domain controller and distribute the final ransomware payload enterprise wide.

Command and Control

- **Bazarbackdoor:**
  - BazarBackdoor is a new malware with the ability to install various types of malicious programs on the infected computers. It is believed to be created by the developers of the TrickBot Trojan, a banking Trojan infecting Windows machines. This is because BazarBackdoor exhibits code and other similarities with TrickBot Trojan.
  - Report_Print.exe
  - 3.137.182.114:443
  - cstr3.com
- **Cobalt Strike:**
  - Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.
  - servisses.exe
  - 88.119.171.94:443
  - Certificate [86:77:d8:5e:51:69:ac:e2:08:07:2e:b0:dc:6c:10:9e:25:80:70:a6]
  - Not Before 2020/10/06 13:33:55 UTC
  - Not After 2021/10/06 13:33:55 UTC
  - Issuer Org lol
  - Subject Common havemosts.com
  - Subject Org lol
  - Public Algorithm rsaEncryption
  - JA3: 57f3642b4e37e28f5cbe3020c9331b4c

- JA3s: e35df3e00ca4ef31d42b34bebaa2f86e
- SQL.dll
- 5.2.64.174:443
- Certificate [36:d5:68:f9:be:2a:34:e1:76:3d:89:78:e5:62:4d:fc:ae:02:97:ad]
- Not Before 2020/10/02 16:45:57 UTC
- Not After 2021/10/02 16:45:57 UTC
- Issuer Org lol
- Subject Common quwasd.com
- Subject Org lol
- Public Algorithm rsaEncryption
- JA3: a0e9f5d64349fb13191bc781f81f42e1
- JA3s: ae4edc6faf64d08308082ad26be60767

Impact

- **Compromise entire network**
  - https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
  - Starting around 4.5 hours after the initial Bazar malware was executed, the Ryuk threat actors acted on their final objectives and initiated RDP connections from the domain controller previously exploited, to the rest of the environment. This time they initiated the ransomware first on the secondary domain controller (their 1st pivot) and transferred the Ryuk executable over the RDP connection.
  - Ryuk is a Ransomware — a type of malware that encrypts files of the victim and restores access in exchange for a ransom payment
  - Based on observed transactions to known Ryuk BTC addresses, the ransom demand varies significantly. This suggests that WIZARD SPIDER (like INDRIK SPIDER with BitPaymer) calculates the ransom amount based on the size and value of the victim organization. To date, the lowest observed ransom was for 1.7 BTC and the highest was for 99 BTC. With 52 known transactions spread across 37 BTC addresses (as of this writing), WIZARD SPIDER has made 705.80 BTC, which has a current value of $3.7 million (USD). With the recent decline in BTC to USD value, it is likely GRIM SPIDER has netted more. The tables in the Appendix include a set of known Ryuk BTC addresses extracted from Ryuk binaries, which are believed to be only a subset of the Ryuk BTC addresses.

```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but
not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
KurtSchweickardt@protonmail.com
or
KurtSchweickardt@tutanota.com

BTC wallet:
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk

Ryuk
No system is safe
```