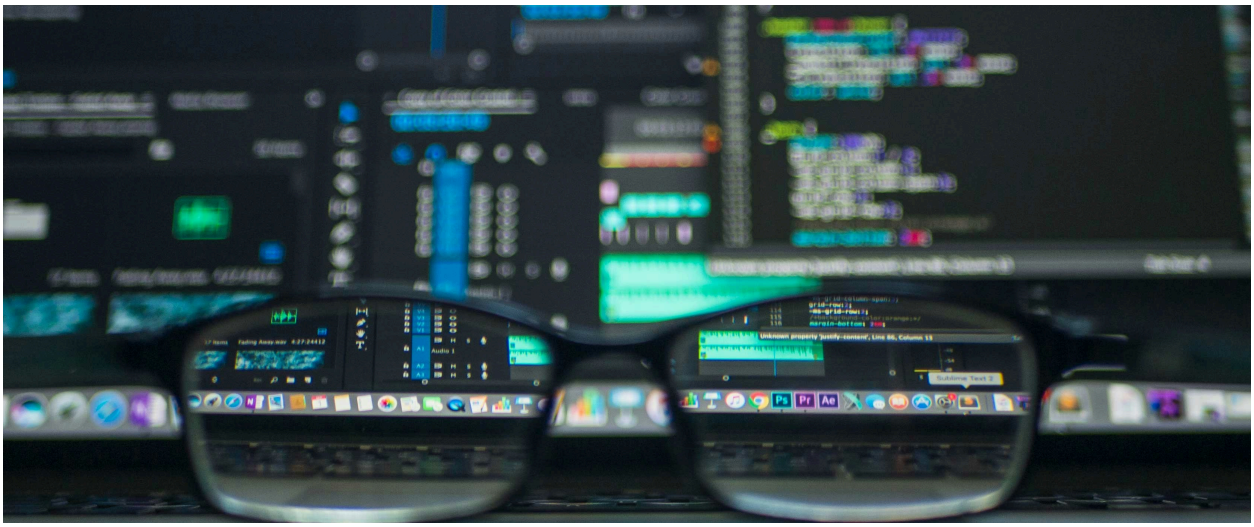


Human-Operated Ransomware: Pre-Attack Behaviors, Tradecraft, and Detection Windows

Define Ransomware

Ransomware is a type of extortion attack that destroys or encrypts files and folders, preventing access to critical data or disrupting critical business systems.

Types of Ransomware:

There are two types of ransomware:

1. **Commodity ransomware** is malware that spreads with phishing or between devices and encrypts files before demanding a ransom.

   e.g. WannaCry or NotPetya

2. **Human-operated ransomware** is a planned and coordinated attack by active cybercriminals who employ multiple attack methods. In many cases, known techniques and tools are used to infiltrate your organization, find the assets or systems worth extorting, and then demand a ransom. Upon compromising a network, the attacker carries out reconnaissance of assets and systems which

can be encrypted or extorted. The attackers then encrypt or exfiltrate data before demanding a ransom.

Human-operated ransomware [the idea behind]

Because human-operated ransomware is typically performed by active attackers who might be performing the steps to infiltrate and discover your most valuable data and systems in real time, the time taken to detect ransomware attacks is crucial.

If pre-ransom activities are detected quickly, the likelihood of a severe attack decreases. The pre-ransom stage typically includes the following techniques:

1. **initial access**
    - RDP brute force
    - Vulnerable internet-facing system
    - Weak application settings
    - Phishing email
2. **reconnaissance**
    - Active Scanning
    - Scanning IP Blocks
    - Vulnerability Scanning
    - Wordlist Scanning
    - Hardware/Software/Firmware details
    - Victim Host Information
3. **credential theft**
    - Mimikatz
    - LSA secrets
    - Credential vault
    - Credentials in plaintext

    - Abuse of service accounts
4. **lateral movement**, and
    - Cobalt Strike
    - WMI
    - Abuse of management tools
    - PsExec
5. **persistence**
    - New accounts
    - GPO changes
    - Shadow IT tools
    - Schedule tasks
    - Service registration

Additionally,

Defense evasion

- Disabling security features
- Clearing log files
- Deleting attack artifact files
- Resetting timestamps on altered files

Exfiltration

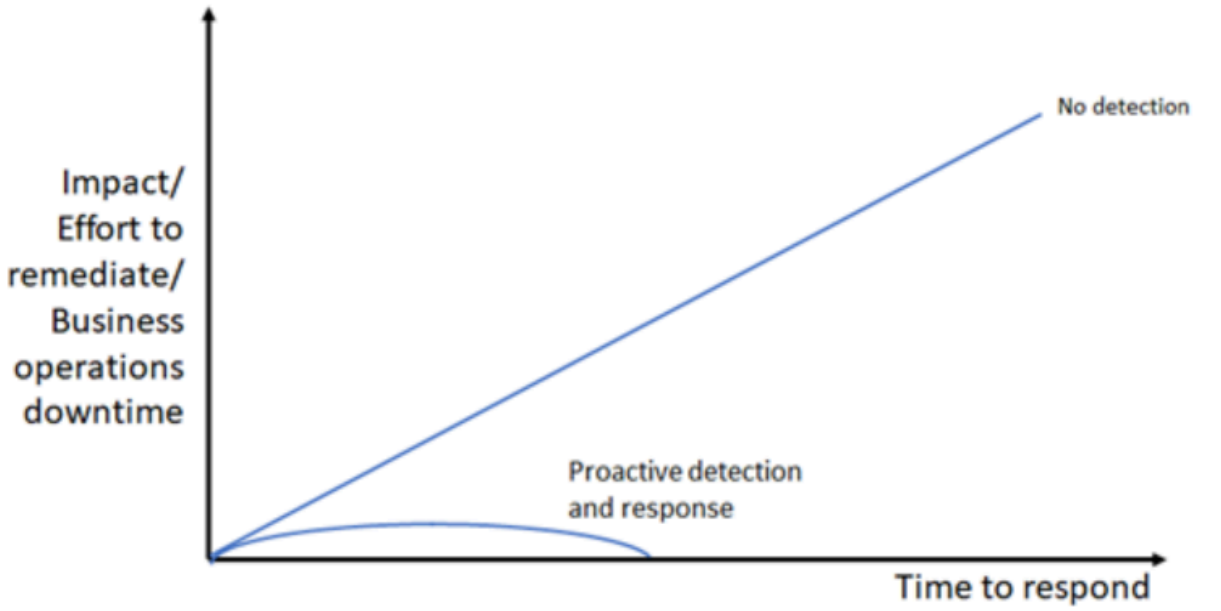
- Exfiltration of sensitive data Impact (financial leverage):
- Encryption of data in place and in backups
- Deletion of data in place and backups, which might be combined with a preceding exfiltration
- Threat of public leakage of exfiltrated, sensitive data

These techniques can initially seem unrelated and often fly under the radar. But if these techniques lead to the ransom stage, it's often too late.

- When detected during the pre-ransom stage, smaller-scale mitigations such as isolating infected devices or user accounts can be used to disrupt and remediate the attack.
- If detection comes at a later stage, such as when the malware used to encrypt files is being deployed, more aggressive remediation steps that can cause downtime might need to be used to disrupt and remediate the attack.

Its never recommend paying a ransom. Paying cybercriminals to get a ransomware decryption key provides no guarantee that your encrypted data will be restored.

Qualitative relationship of the impact of a ransomware attack and your time to respond for no detection vs. proactive detection and response:



Being familiar with pre-ransom malware, payloads, and activities helps analysts know what to look for to prevent the later stages of an attack.

The challenge for security analysts is recognizing when an alert is part of a larger attack chain with the goal of extorting your sensitive data or crucial systems.

Human-operated ransomware campaigns often start with “commodity malware” like banking Trojans or “unsophisticated” attack vectors that typically trigger multiple detection alerts; however, these tend to be triaged as unimportant and

therefore not thoroughly investigated and remediated. In addition, the initial payloads are frequently stopped by antivirus solutions, but attackers just deploy a different payload or use administrative access to disable the antivirus without attracting the attention of incident responders or security operations centers (SOCs).

Some well-known human-operated ransomware campaigns include REvil, Samas, Bitpaymer, and Ryuk. Microsoft actively monitors these and other long-running human-operated ransomware campaigns, which have overlapping attack patterns. They take advantage of similar security weaknesses, highlighting a few key lessons in security, notably that these attacks are often preventable and detectable.

Case Studies...

1. PARINACOTA group: Smash-and-grab monetization campaigns

One actor that has emerged in this trend of human-operated attacks is an active, highly adaptive group that frequently drops Wadhrama as payload. Microsoft has been tracking this group for some time, but now refers to them as PARINACOTA, using their new naming designation for digital crime actors based on global volcanoes.

Microsoft's naming system:

> Microsoft recently updated their threat actor naming taxonomy and now uses **volcano names** to designate digital crime/cybercrime groups. This is why they chose "PARINACOTA" (after the Andean volcano) as the designation for this particular ransomware group.
>
> This naming approach helps Microsoft organize and communicate about different threat actors systematically. They use different naming themes for different categories:
>
> - Volcanoes for cybercrime groups
> - Weather patterns for nation-state actors
> - Elements for other categories

Wadhrama (also known as **Dharma** or **Crysis**) is a ransomware family that has been active since 2016.

Classification & Aliases:

- Primary names: Dharma, Crysis, Wadhrama Palo Alto Networks
- Additional aliases: Arena, ncov Malpedia
- Microsoft detection: Ransom:Win32/Wadhrama
- Type: File-encrypting ransomware with RaaS (Ransomware-as-a-Service) model

Primary Distribution Methods:

- Manual installation by attackers via compromised Remote Desktop Protocol (RDP) services, typically on TCP port 3389 Malpedia
- Malicious attachments in phishing emails and disguised installers appearing to be legitimate software such as antivirus Palo Alto Networks
- Social engineering tactics
- Often appears alongside HackTool:Win32/AutoKMS (KMS activation tools) Microsoft

Attack Pattern:

- Attackers scan the internet for exposed RDP services, then attempt brute-force attacks on credentials to gain initial access.

Installation Phase:

The malware copies itself to the Windows System folder and Start Menu Startup folder, maintaining its original filename.

File Locations:

- `%System%\<malware_filename>.exe` (typically C:\Windows\System32)
- `%User Startup%\<malware_filename>.exe`
- `%AppData%\<malware_filename>.exe`

Persistence Mechanisms:

Creates registry Run keys for automatic execution at system startup
Registry Modifications:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Key: "<malware filename>" (e.g., test6.exe)
Value: "%system%\<malware filename>"

HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Key: "{Malware Filename}.exe"
Value: "%Application Data%\{Malware Filename}.exe"
```

Defense Evasion:

Deletes shadow copy backups to prevent file recovery

- Reads data from its own binary image containing encrypted or compressed code to evade antivirus detection

Target Scope:
Encrypts most files on the C:\ drive and other attached disks, excluding directories containing "Windows" or "Microsoft" in their names

- Also attempts to encrypt files on network shares
- Targets multiple drives simultaneously

File Naming Convention:
Appends extensions like [makedonskiy@india.com].wallet to encrypted filenames

The email address in the extension varies by variant and is used as the contact point for ransom payment.

Binary Properties:

- File Type: Windows PE executable (.exe)
- File Size: Varies (94,720 - 200,704 bytes reported across variants)
- Memory Resident: Yes
- Platform: Windows (all versions, though Windows 7 was significantly more vulnerable)

Behavioral Indicators:

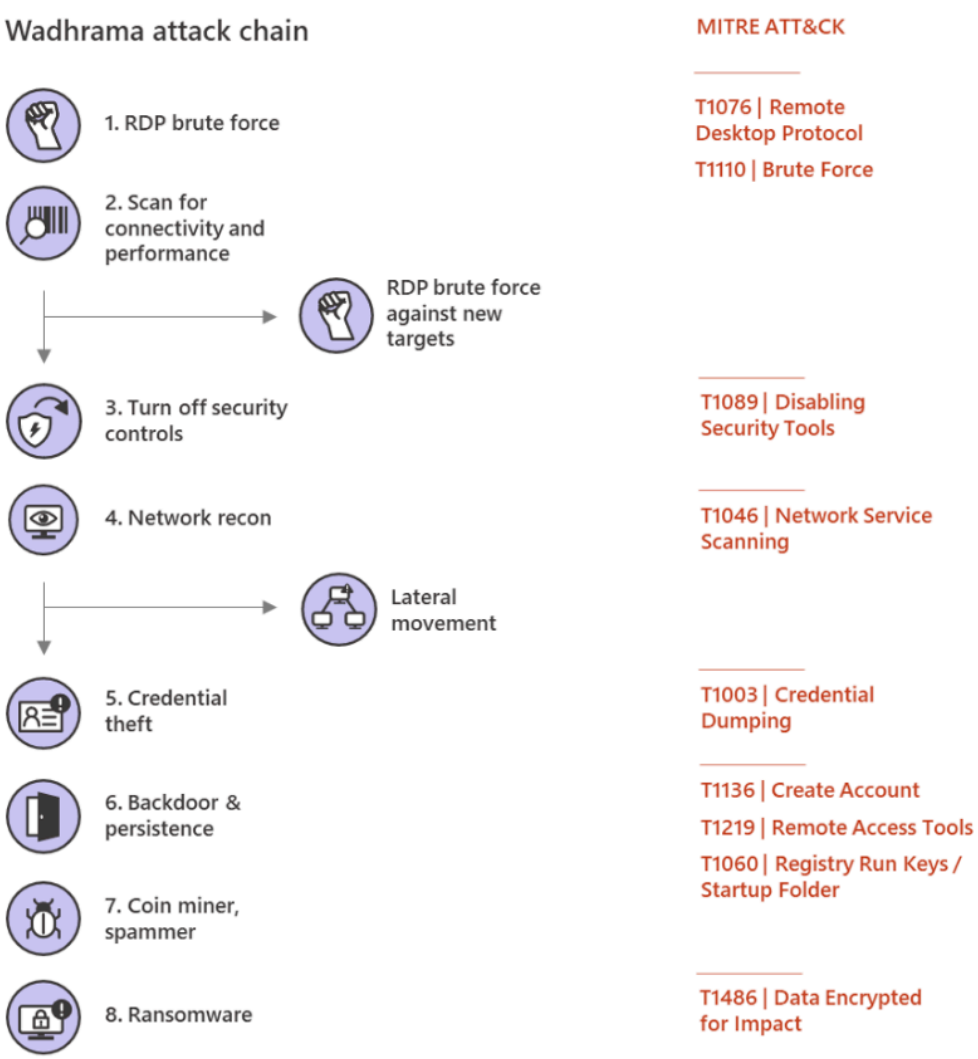
- Installs itself for autorun using the Windows startup folder at C:\Users[user-name]\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup Howtofix
- Drops ransom notes on the desktop and in encrypted directories
- May display false alerts about unlicensed software or illegal content to pressure victims

---

The group most often employs a smash-and-grab method, whereby they attempt to infiltrate a machine in a network and proceed with subsequent ransom in less than an hour. There are outlier campaigns in which they attempt reconnaissance and lateral movement, typically when they land on a machine and network that allows them to quickly and easily move throughout the environment.

PARINACOTA's attacks typically brute forces their way into servers that have Remote Desktop Protocol (RDP) exposed to the internet, with the goal of moving laterally inside a network or performing further brute-force activities against targets outside the network. This allows the group to expand compromised infrastructure under their control. Frequently, the group targets built-in local administrator accounts or a list of common account names. In other instances, the group targets Active Directory (AD) accounts that they compromised or have prior knowledge of, such as service accounts of known vendors.

The group adopted the RDP brute force technique that the older ransomware called Samas (also known as SamSam) infamously used. Other malware families like GandCrab, MegaCortext, LockerGoga, Hermes, and RobbinHood have also used this method in targeted ransomware attacks. PARINACOTA, however, has also been observed to adapt to any path of least resistance they can utilize. For instance, they sometimes discover unpatched systems and use disclosed vulnerabilities to gain initial access or elevate privileges.



We gained insight into these attacks by investigating compromised infrastructure that the group often utilizes to proxy attacks onto their next targets. To find targets, the group scans the internet for machines that listen on RDP port 3389. The attackers do this from compromised machines using tools like *Masscan.exe,* which can find vulnerable machines on the entire internet in under six minutes.

Once a vulnerable target is found, the group proceeds with a brute force attack using tools like *NLbrute.exe* or ForcerX, starting with common usernames like ‘admin’, ‘administrator’, ‘guest’, or ‘test’. After successfully gaining access to a network, the group tests the compromised machine for internet connectivity and processing capacity. They determine if the machine meets certain requirements before using it to conduct subsequent RDP brute force attacks against other

targets. This tactic, which has not been observed being used by similar ransomware operators, gives them access to additional infrastructure that is less likely to be blocked. In fact, the group has been observed leaving their tools running on compromised machines for months on end.

On machines that the group doesn't use for subsequent RDP brute-force attacks, they proceed with a separate set of actions. This technique helps the attackers evade reputation-based detection, which may block their scanning boxes; it also preserves their command-and-control (C2) infrastructure. In addition, PARINACOTA utilizes administrative privileges gained via stolen credentials to turn off or stop any running services that might lead to their detection.

After disabling security solutions, the group often downloads a ZIP archive that contains dozens of well-known attacker tools and batch files for credential theft, persistence, reconnaissance, and other activities without fear of the next stages of the attack being prevented. With these tools and batch files, the group clears event logs using *wevutil.exe*, as well as conducts extensive reconnaissance on the machine and the network, typically looking for opportunities to move laterally using common network scanning tools. When necessary, the group elevates privileges from local administrator to SYSTEM using accessibility features in conjunction with a batch file or exploit-laden files named after the specific CVEs they impact, also known as the "Sticky Keys" attack.

The group dumps credentials from the LSASS process, using tools like Mimikatz and ProcDump, to gain access to matching local administrator passwords or service accounts with high privileges that may be used to start as a scheduled task or service, or even used interactively. PARINACOTA then uses the same remote desktop session to exfiltrate acquired credentials. The group also attempts to get credentials for specific banking or financial websites, using *findstr.exe* to check for cookies associated with these sites.

With credentials on hand, PARINACOTA establishes persistence using various methods, including:

- Registry modifications using .bat or .reg files to allow RDP connections

```
reg  add "HKLM\system\CurrentControlSet\Control\Terminal Server" /v "AllowTSConnections" /t REG_DWORD /d 0x1 /f
reg  add "HKLM\system\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0x0 /f
reg  add "HKLM\system\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "MaxConnectionTime" /t REG_DWORD /d 0x1 /f
reg  add "HKLM\system\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "MaxDisconnectionTime" /t REG_DWORD /d 0x0 /f
reg  add "HKLM\system\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v "MaxIdleTime" /t REG_DWORD /d 0x0 /f
reg  add "HKLM\software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v Adminisrator /t REG_DWORD /d 0x0 /f
```

- Setting up access through existing remote assistance apps or installing a backdoor
- Creating new local accounts and adding them to the local administrators group

```
net  user [redacted] [redacted] /add /active:"yes" /expires:"never" /passwordchg:"NO"
net  localgroup Administrators [redacted] /add
net  localgroup "Remote Desktop Users" [redacted] /add
reg  add "HKLM\software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v [redacted] /t REG_DWORD /d 0x0 /f
```

To determine the type of payload to deploy, PARINACOTA uses tools like Process Hacker to identify active processes. The attackers don't always install ransomware immediately; they have been observed installing coin miners and using *massmail.exe* to run spam campaigns, essentially using corporate networks as distributed computing infrastructure for profit. The group, however, eventually returns to the same machines after a few weeks to install ransomware.

The group performs the same general activities to deliver the ransomware payload:

- Plants a malicious HTA file (*hta* in many instances) using various autostart extensibility points (ASEPs), but often the registry Run keys or the Startup folder. The HTA file displays ransom payment instructions.
- Deletes local backups using tools like *exe* to stifle recovery of ransomed files.
- Stops active services that might interfere with encryption using *exe*, *net.exe*, or other tools.

```
net  stop MSSQLServerADHelper100
net  stop MSSQL$ISARS
net  stop MSSQL$MSFW
net  stop SQLAgent$ISARS
net  stop SQLAgent$MSFW
net  stop SQLBrowser
net  stop ReportServer$ISARS
net  stop SQLWriter
net  stop WinDefend
net  stop mr2kserv
net  stop MSExchangeADTopology
net  stop MSExchangeFBA
net  stop MSExchangeIS
net  stop MSExchangeSA
net  stop ShadowProtectSvc
net  stop SPAdminV4
net  stop SPTimerV4
net  stop SPTraceV4
net  stop SPUserCodeV4
net  stop SPWriterV4
net  stop IISADMIN
net  stop QuickBooksDB15
net  stop QuickBooksDB17
net  stop QuickBooksDB18
net  stop QuickBooksDB21
net  stop QuickBooksDB24
taskkill  /f /im mysql*
taskkill  /f /im IBM*
taskkill  /f /im bes10*
taskkill  /f /im black*
taskkill  /f /im sql
taskkill  /f /im store.exe
taskkill  /f /im sql*
taskkill  /f /im vee*
taskkill  /f /im postg*
taskkill  /f /im sage*
```

- Drops an array of malware executables, often naming the files based on their intended behavior. If previous attempts to stop antivirus software have been unsuccessful, the group simply drops multiple variants of a malware until they manage to execute one that is not detected, indicating that even when detections and alerts are occurring, network admins are either not seeing them or not reacting to them.

As mentioned, PARINACOTA has recently mostly dropped the Wadhrama ransomware, which leaves the following ransom note after encrypting target files:

In several observed cases, targeted organizations that were able to resolve ransomware infections were unable to fully remove persistence mechanisms, allowing the group to come back and deploy ransomware again.

PARINACOTA routinely uses Monero coin miners on compromised machines, allowing them to collect uniform returns regardless of the type of machine they access. Monero is popular among cybercriminals for its privacy benefits: Monero not only restricts access to wallet balances, but also mixes in coins from other transactions to help hide the specifics of each transaction, resulting in transactions that aren't as easily traceable by amount as other digital currencies.

As for the ransomware component, we have seen reports of the group charging anywhere from .5 to 2 Bitcoins per compromised machine. This varies depending on what the attackers know about the organization and the assets that they have compromised. The ransom amount is adjusted based on the likelihood the organization will pay due to impact to their company or the perceived importance of the target.

2. Doppelpaymer: Ransomware follows Dridex

Doppelpaymer ransomware recently caused havoc in several highly publicized attacks against various organizations around the world. Some of these attacks involved large ransom demands, with attackers asking for millions of dollars in some cases.

Doppelpaymer ransomware, like Wadhrama, Samas, LockerGoga, and Bitpaymer before it, does not have inherent worm capabilities. Human operators manually spread it within compromised networks using stolen credentials for privileged accounts along with common tools like PsExec and Group Policy. They often abuse service accounts, including accounts used to manage security products, that have domain admin privileges to run native commands, often stopping antivirus software and other security controls.

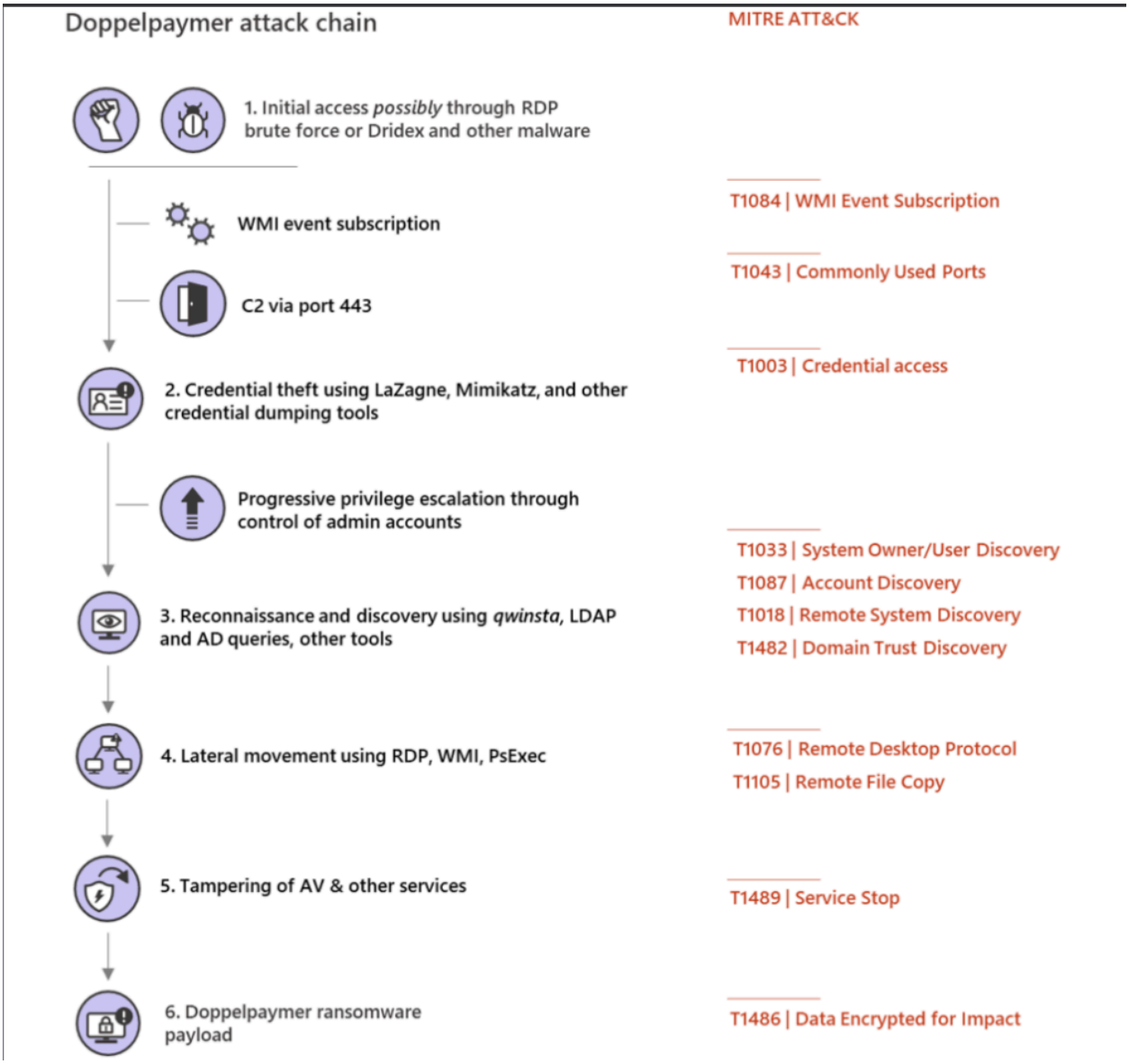
The presence of banking Trojans like Dridex on machines compromised by Doppelpaymer point to the possibility that Dridex (or other malware) is introduced during earlier attack stages through fake updaters, malicious documents in phishing email, or even by being delivered via the Emotet botnet.

While Dridex is likely used as initial access for delivering Doppelpaymer on machines in affected networks, most of the same networks contain artifacts indicating RDP brute force. This is in addition to numerous indicators of credential theft and the use of reconnaissance tools. Investigators have in fact found artifacts indicating that affected networks have been compromised in some manner by various attackers for several months before the ransomware is deployed, showing that these attacks (and others) are successful and unresolved in networks where diligence in security controls and monitoring is not applied.

The use of numerous attack methods reflects how attackers freely operate without disruption – even when available endpoint detection and response (EDR) and endpoint protection platform (EPP) sensors already detect their activities. In many cases, some machines run without standard safeguards, like security updates and cloud-delivered antivirus protection. There is also the lack of credential hygiene, over-privileged accounts, predictable local administrator and RDP passwords, and unattended EDR alerts for suspicious activities.

The success of attacks relies on whether campaign operators manage to gain control over domain accounts with elevated privileges after establishing initial access. Attackers utilize various methods to gain access to privileged accounts,

including common credential theft tools like Mimikatz and LaZagne. Microsoft has also observed the use of the Sysinternals tool ProcDump to obtain credentials from LSASS process memory. Attackers might also use LSASecretsView or a similar tool to access credentials stored in the LSA secrets portion of the registry. Accessible to local admins, this portion of the registry can reveal credentials for domain accounts used to run scheduled tasks and services.



Doppelpaymer infection chain

Campaign operators continually steal credentials, progressively gaining higher privileges until they control a domain administrator-level account. In some cases,

operators create new accounts and grant Remote Desktop privileges to those accounts.

Apart from securing privileged accounts, attackers use other ways of establishing persistent access to compromised systems. In several cases, affected machines are observed launching a base64-encoded PowerShell Empire script that connects to a C2 server, providing attackers with persistent control over the machines. Limited evidence suggests that attackers set up WMI persistence mechanisms, possibly during earlier breaches, to launch PowerShell Empire.

After obtaining adequate credentials, attackers perform extensive reconnaissance of machines and running software to identify targets for ransomware delivery. They use the built-in command *qwinsta* to check for active RDP sessions, run tools that query Active Directory or LDAP, and ping multiple machines. In some cases, the attackers target high-impact machines, such as machines running systems management software. Attackers also identify machines that they could use to stay persistent on the networks after deploying ransomware.

Attackers use various protocols or system frameworks (WMI, WinRM, RDP, and SMB) in conjunction with PsExec to move laterally and distribute ransomware. Upon reaching a new device through lateral movement, attackers attempt to stop services that can prevent or stifle successful ransomware distribution and execution. As in other ransomware campaigns, the attackers use native commands to stop Exchange Server, SQL Server, and similar services that can lock certain files and disrupt attempts to encrypt them. They also stop antivirus software right before dropping the ransomware file itself.

Attempts to bypass antivirus protection and deploy ransomware are particularly successful in cases where:

- Attackers already have domain admin privileges
- Tamper protection is off
- Cloud-delivered protection is off
- Antivirus software is not properly managed or is not in a healthy state

Microsoft Defender ATP generates alerts for many activities associated with these attacks. However, in many of these cases, affected network segments and their associated alerts are not actively being monitored or responded to.

Attackers also employ a few other techniques to bypass protections and run ransomware code. In some cases, investigators found artifacts indicating that they introduce a legitimate binary and use Alternate Data Streams to masquerade the execution of the ransomware binary as legitimate binary.

```
C:\Users\user\AppData\Roaming>dir /R IXRCWJ
Volume in drive C has no label.
Volume Serial Number is 5EFA-295B


Directory of C:\Users\user\AppData\Roaming


01/22/2020 03:38 PM           15,872 IXRCWJ
181,248 IXRCWJ:nHv3:$DATA
1 File(s)         15,872 bytes
0 Dir(s) 14,206,267,392 bytes free


C:\Users\user\AppData\Roaming>xxd -l 128 < IXRCWJ:nHv3
00000000: 4d5a 9000 0300 0000 0400 0000 ffff 0000 MZ..............
00000010: b800 0000 0000 0000 4000 0000 0000 0000 ........@.......
00000020: 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000030: 0000 0000 0000 0000 0000 0000 f800 0000 ................
00000040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468 ........!..L.!Th
00000050: 6973 2070 726f 6772 616d 2063 616e 6e6f is program canno
00000060: 7420 6265 2072 756e 2069 6e20 444f 5320 t be run in DOS
00000070: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000 mode....$.....
```

Command prompt dump output of the Alternate Data Stream

The Doppelpaymer ransomware binary used in many attacks are signed using what appears to be stolen certificates from *OFFERS CLOUD LTD*, which might be trusted by various security solutions.

Doppelpaymer encrypts various files and displays a ransom note. In observed cases, it uses a custom extension name for encrypted files using information about the affected environment. For example, it has used *l33tspeak* versions of company names and company phone numbers.

Notably, Doppelpaymer campaigns do not fully infect compromised networks with ransomware. Only a subset of the machines have the malware binary and a slightly smaller subset have their files encrypted. The attackers maintain persistence on machines that don't have the ransomware and appear intent to use these machines to come back to networks that pay the ransom or do not perform a full incident response and recovery.

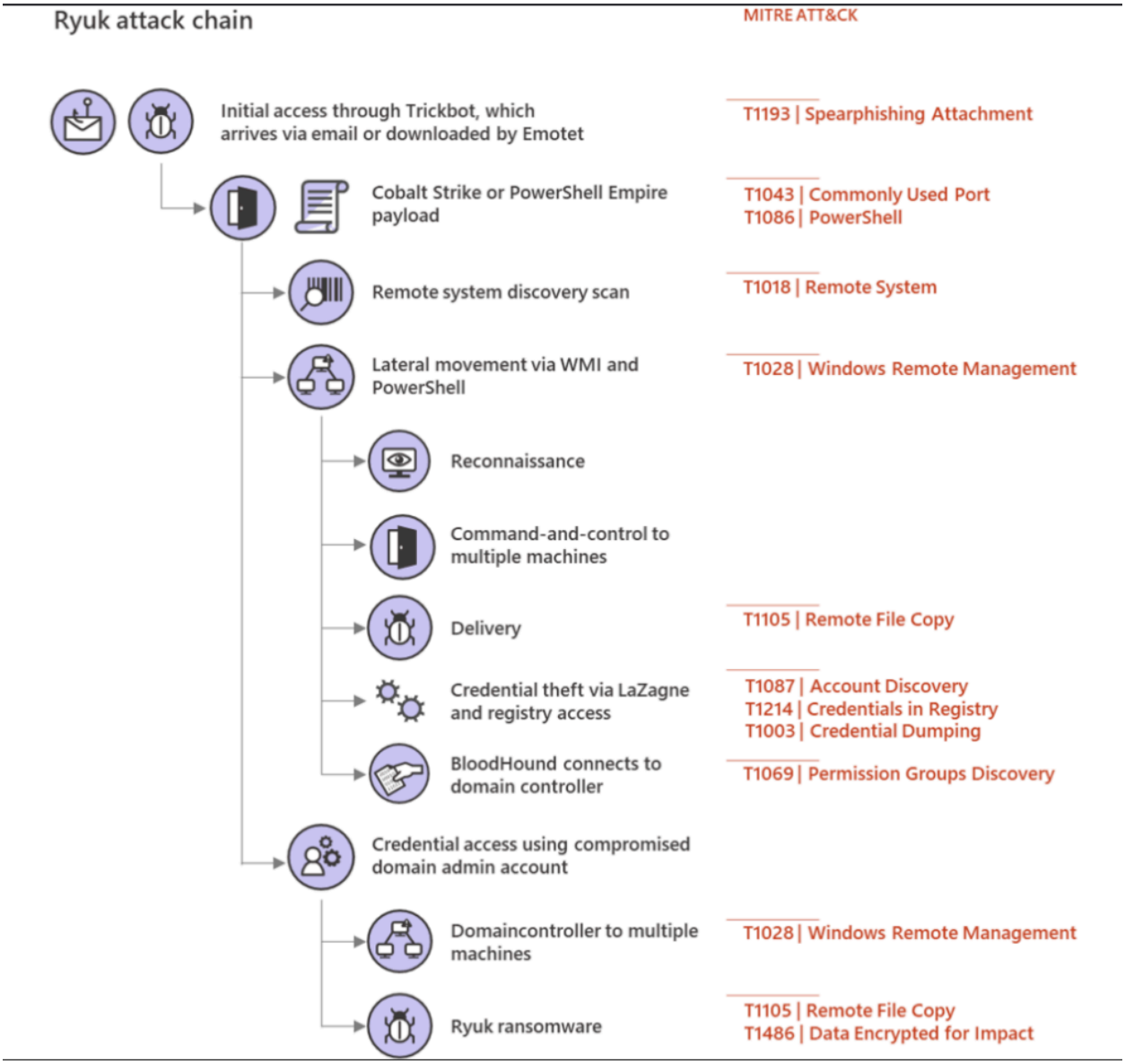
3. Ryuk: Human-operated ransomware initiated from Trickbot infections

Ryuk is another active human-operated ransomware campaign that wreaks havoc on organizations, from corporate entities to local governments to non-profits by disrupting businesses and demanding massive ransom. Ryuk originated as a ransomware payload distributed over email, and but it has since been adopted by human operated ransomware operators.

Like Doppelpaymer, Ryuk is one of possible eventual payloads delivered by human operators that enter networks via banking Trojan infections, in this case Trickbot. At the beginning of a Ryuk infection, an existing Trickbot implant downloads a new payload, often Cobalt Strike or PowerShell Empire, and begins to move laterally across a network, activating the Trickbot infection for ransomware deployment. The use of Cobalt Strike beacon or a PowerShell Empire payload gives operators more maneuverability and options for lateral movement on a network. Based on investigations, in some networks, this may also provide the added benefit to the attackers of blending in with red team activities and tools.

Investigations have found that this activation occurs on Trickbot implants of varying ages, indicating that the human operators behind Ryuk likely have some sort of list of check-ins and targets for deployment of the ransomware. In many cases, however, this activation phase comes well after the initial Trickbot infection, and the eventual deployment of a ransomware payload may happen weeks or even months after the initial infection.

In many networks, Trickbot, which can be distributed directly via email or as a second-stage payload to other Trojans like Emotet, is often considered a low-priority threat, and not remediated and isolated with the same degree of scrutiny as other, more high-profile malware. This works in favor of attackers, allowing them to have long-running persistence on a wide variety of networks. Trickbot, and the Ryuk operators, also take advantage of users running as local administrators in environments and use these permissions to disable security tools that would otherwise impede their actions.



Ryuk infection chain

Once the operators have activated on a network, they utilize their Cobalt Strike or PowerShell tools to initiate reconnaissance and lateral movement on a network. Their initial steps are usually to use built-in commands such as net group to enumerate group membership of high-value groups like domain administrators and enterprise administrators, and to identify targets for credential theft.

Ryuk operators then use a variety of techniques to steal credentials, including the LaZagne credential theft tool. The attackers also save various registry hives to extract credentials from Local Accounts and the LSA Secrets portion of the registry that stores passwords of service accounts, as well as Scheduled Tasks configured to auto start with a defined account. In many cases, services like security and systems management software are configured with privileged accounts, such as domain administrator; this makes it easy for Ryuk operators to migrate from an initial desktop to server-class systems and domain controllers. In addition, in many environments successfully compromised by Ryuk, operators are able to utilize the built-in administrator account to move laterally, as these passwords are matching and not randomized.

Once they have performed initial basic reconnaissance and credential theft, the attackers in some cases utilize the open source security audit tool known as BloodHound to gather detailed information about the Active Directory environment and probable attack paths. This data and associated stolen credentials are accessed by the attacker and likely retained, even after the ransomware portion is ended.

The attackers then continue to move laterally to higher value systems, inspecting and enumerating files of interest to them as they go, possibly exfiltrating this data. The attackers then elevate to domain administrator and utilize these permissions to deploy the Ryuk payload.

The ransomware deployment often occurs weeks or even months after the attackers begin activity on a network. The Ryuk operators use stolen Domain Admin credentials, often from an interactive logon session on a domain controller, to distribute the Ryuk payload. They have been seen doing this via Group Policies, setting a startup item in the SYSVOL share, or, most commonly in recent attacks, via PsExec sessions emanating from the domain controller itself.

References:

Microsoft

- https://learn.microsoft.com/en-us/defender-xdr/playbook-detecting-ransomware-m365-defender
- https://www.microsoft.com/en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/