datto

Wizard Spider Threat Profile

Wizard Spider (Crowdstrike), UNC1878 (FireEye), Team9

Table of Contents

Motives

Tactics, Techniques, and Procedures

Mitigations/ Defenses

Detection Opportunities

Resources

Wizard Spider are a sophisticated organized cybercrime group that was originally known for the development and operation of the Trickbot malware in 2016. Since then, Wizard Spider has become notorious for the development and operation of the Ryuk ransomware.

Wizard Spider performs low-frequency, targeted ransomware campaigns with high ransom demands, known as Big Game Hunting. Wizard Spider are one of the most successful cybercrime groups in operation, and in 2020, cryptocurrency wallets linked to Ryuk received almost $100 million USD in victim payments.

Motives

Wizard Spider is financially motivated. Almost every malware developed by the group is designed to steal or encrypt sensitive information for monetary gain.

Tactics, Techniques, and Procedures (TTPs)

Wizard Spider-attributed attacks show a consistent, methodical approach to the actor's tactics, techniques, and procedures (TTPs).

Since the disruption of Emotet by Europol and Eurojust in early 2021, Wizard Spider have moved from their well-known Emotet -> Trickbot -> Ryuk attack chain to utilizing other commodity malware while mostly keeping the same tactics and techniques.

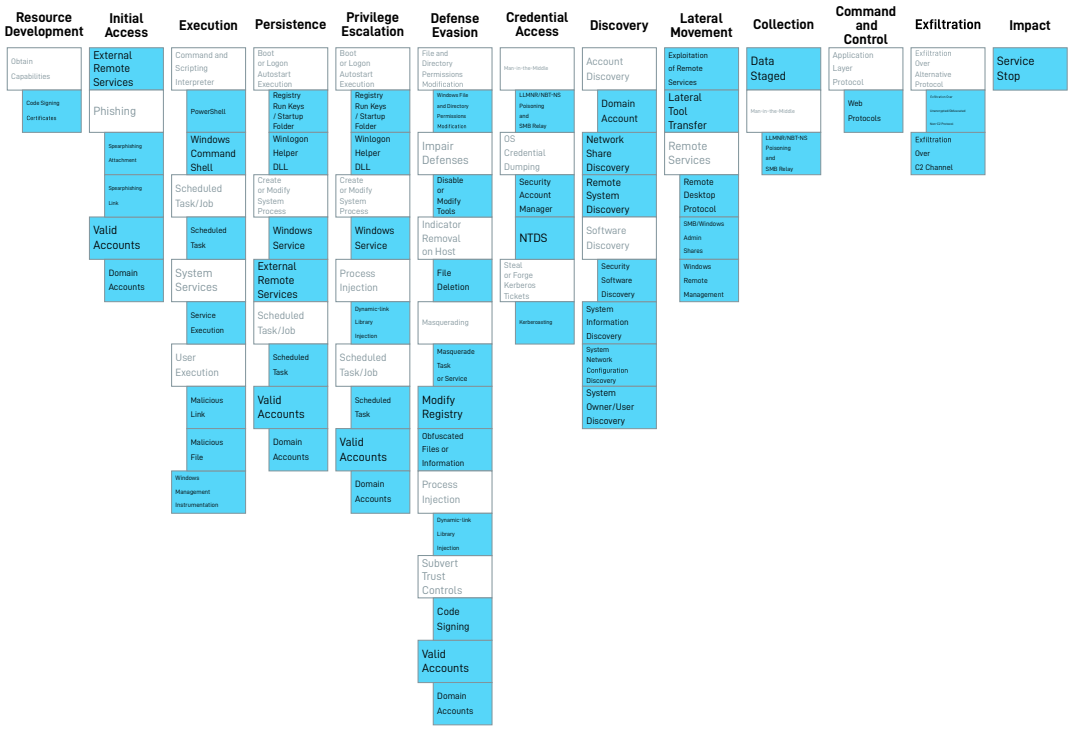
One of Wizard Spider's methods for initial access is via phishing email campaigns with a malicious document attached. Most recently, Wizard Spider has been attributed to the exploitation of CVE-2021-40444, which used malicious documents to exploit a vulnerability in MSHTML to download and execute malware on victim devices.

If a user opens the attachment and activates the document's macros, a 'dropper' malware is installed onto the victim device. The dropper will then establish communications with its Command and Control (C2) server and load a more full-featured malware onto the device as the second stage of the attack..

Once the second stage malware has established itself on the victim device, Wizard Spider will begin network reconnaissance and bring down additional tooling & malware to perform network reconnaissance, lateral movement, and privilege escalation. Wizard Spider will target getting access to the network's domain controllers before finally deploying Ryuk to the network.

MITRE ATT&CK:

The following lists Wizard Spider's known TTPs mapped to MITRE ATT&CK:



Initial Access

- **Phishing: Spearphishing Attachment (T1566.001) -** Wizard Spider has used spearphishing attachments to deliver malicious documents with macros or PDFs containing malicious links to download malware.
- **Phishing: Spearphishing Link (T1566.002) -** Wizard Spider has sent phishing emails containing a link to an actor-controlled document hosted on online file hosting services.

Execution

- **Command and Scripting Interpreter: PowerShell (T1059.001) -** Wizard Spider has executed PowerShell scripts via document macros to download malware onto the victim's machines.
- **Command and Scripting Interpreter: Windows Command Shell (T1059.003) -** Wizard Spider has used cmd.exe to execute commands on a victim's machine.
- **User Execution: Malicious File (T1204.002) -** Wizard Spider has relied on victims to execute malware with spearphishing attachments containing malicious macros.
- **User Execution: Malicious Link (T1204.001) -** Wizard Spider has relied on victims to click on malicious links in spearphishing emails.

Table of Contents

Motives

Tactics, Techniques, and Procedures

Mitigations/ Defenses

Detection Opportunities

Resources

Table of Contents

Motives

Tactics, Techniques, and Procedures

Mitigations/ Defenses

Detection Opportunities

Resources

Persistence

- **Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder (T1547.001) -** Wizard Spider has established persistence via the Registry run key HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, as well as a shortcut within the startup folder.
- **Scheduled Task/Job: Scheduled Task (T1053.005) -** Wizard Spider has used scheduled tasks to establish persistence.

Defense Evasion

- **Obfuscated Files or Information (T1027) -** Wizard Spider used Base64 encoding to obfuscate PowerShell commands.
- **Process Injection: Dynamic-link Library Injection (T1055.001) -** Wizard Spider has injected malicious DLLs into memory with read, write, and execute permissions.

Credential Access

- **Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003) -** Wizard Spider has used Rubeus, the MimiKatz Kerberos module, and the Invoke-Kerberoast cmdlet to steal AES hashes.

Discovery

- **Account Discovery: Domain Account (T1087.002) -** Wizard Spider has used the "net group 'Domain admins'" command to identify domain admins.
- **Network Share Discovery (T1135) -** Wizard Spider has used the "net view" command to locate mapped network shares.
- **Software Discovery: Security Software Discovery (T1518.001) -** Wizard Spider has used WMI to identify antivirus products installed on a victim's device.
- **Remote System Discovery (T1018) -** Wizard Spider has used networkdll, psfin, nltest, and dclist for remote system and domain discovery.

Lateral Movement

- **Exploitation of Remote Services (T1210) -** Wizard Spider has exploited, or attempted to exploit, software vulnerabilities to move laterally in networks.
- **Remote Services: SMB/Windows Admin Shares (T1021.002) -** Wizard Spider has used SMB to drop Cobalt Strike Beacon on a domain controller for lateral movement.
- Command and Control
- **Application Layer Protocol: Web Protocols (T1071.001) -** Wizard Spider has used HTTP for network communications.

Exfiltration

- **Exfiltration Over C2 Channel (T1041) -** Wizard Spider has exfiltrated domain credentials and network enumeration information over command and control (C2) channels.

Impact

- **Service Stop (T1489) -** Wizard Spider stopped services prior to network encryption.
- **Inhibit System Recovery (T1490) -** Wizard Spider has deleted volume shadow copies before encrypting victim devices with Ryuk.
- **Data Encrypted for Impact (T1486) -** Wizard Spider has encrypted victim devices using Ryuk ransomware.

Table of Contents

Motives

Tactics, Techniques, and Procedures

Mitigations/ Defenses

Detection Opportunities

Resources

Mitigations/Defenses

It is recommended to implement a strong foundation of security controls in order to defend your network against the LockBit threat actors.

The Center for Internet Security (CIS) Controls are a prioritized set of actions designed to defend against cyber attacks and threat actors. The CIS Controls have three tiers, known as Implementation Groups, that build on each other.

The following table maps Wizard Spider's MITRE ATT&CK techniques to CIS v8 Safeguards:

MITRE ATT&CK	CIS Safeguards
Phishing: Spearphishing Attachment (T1566.001)	**IG1** 2.3: Address Unauthorized Software 14.1: Establish and Maintain a Security Awareness Program 14.2: Train Workforce Members to Recognize Social Engineering Attacks 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents
Phishing: Spearphishing Link (T1566.002)	**IG1** 2.3: Address Unauthorized Software 14.1: Establish and Maintain a Security Awareness Program 14.2: Train Workforce Members to Recognize Social Engineering Attacks 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents
Command and Scripting Interpreter: PowerShell (T1059.001)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 10.1: Deploy and Maintain Anti-Malware Software 10.2: Configure Automatic Anti-Malware Signature Updates
Command and Scripting Interpreter: Windows Command Shell (T1059.003)	**IG2** 2.5: Allowlist Authorized Software **IG3** 2.7: Allowlist Authorized Scripts
User Execution: Malicious File (T1204.002)	**IG1** 14.1: Establish and Maintain a Security Awareness Program 14.2: Train Workforce Members to Recognize Social Engineering Attacks 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents

— IG1 — IG2 — IG3

Table of Contents

Motives

Tactics, Techniques, and Procedures

Mitigations/ Defenses

Detection Opportunities

Resources

User Execution: Malicious Link (T1204.001)	**IG1** 14.1: Establish and Maintain a Security Awareness Program 14.2: Train Workforce Members to Recognize Social Engineering Attacks 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents
Scheduled Task/Job: Scheduled Task (T1053.005)	**IG1** 6.2: Establish an Access Revoking Process 8.3: Ensure Adequate Audit Log Storage
Obfuscated Files or Information (T1027)	**IG1** 10.1: Deploy and Maintain Anti-Malware Software 10.2: Configure Automatic Anti-Malware Signature Updates
Process Injection: Dynamic-link Library Injection (T1055.001)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process
Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.2: Use Unique Passwords 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts
Account Discovery: Domain Account (T1087.002)	**IG1** Establish and Maintain a Secure Configuration Process
Network Share Discovery (T1135)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process
Exploitation of Remote Services (T1210)	**IG1** 2.3: Address Unauthorized Software 4.1: Establish and Maintain a Secure Configuration Process 4.4: Implement and Manage a Firewall on Servers 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 7.1: Establish and Maintain a Vulnerability Management Process 7.2: Establish and Maintain a Remediation Process 7.3: Perform Automated Operating System Patch Management 7.4: Perform Automated Application Patch Management

— IG1 — IG2 — IG3

Table of Contents

Motives

Tactics, Techniques, and Procedures

Mitigations/ Defenses

Detection Opportunities

Resources

Remote Services: SMB/ Windows Admin Shares (T1021.002)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers 4.5: Implement and Manage a Firewall on End-User Devices 4.7: Manage Default Accounts on Enterprise Assets and Software 5.2: Use Unique Passwords 5.3: Disable Dormant Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process
Application Layer Protocol: Web Protocols (T1071.001)	**IG2** 13.3: Deploy a Network Intrusion Detection Solution **IG3** 13.8: Deploy a Network Intrusion Prevention Solution
Exfiltration Over C2 Channel (T1041)	**IG2** 13.3: Deploy a Network Intrusion Detection Solution **IG3** 13.8: Deploy a Network Intrusion Prevention Solution
Service Stop (T1489)	**IG1** 3.12: Segment Data Processing and Storage Based on Sensitivity 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process
Inhibit System Recovery (T1490)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data
Data Encrypted for Impact (T1486)	**IG1** 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data

— IG1 — IG2 — IG3

Table of Contents

Motives

Tactics, Techniques, and Procedures

Mitigations/ Defenses

Detection Opportunities

Resources

Detection Opportunities

Detecting Wizard Spider's activities requires mapping their known attack vectors to actionable defensive controls and validating your defenses through reliable, repeatable testing.

The following detection opportunities are mapped to MITRE ATT&CK v9 techniques, CIS v8 safeguards, and provide appropriate Red Canary Atomic Red Team tests to undertake for validation:

Detection Opportunity 1: Detecting Shadow Copy Deletion

MITRE ATT&CK: Inhibit System Recovery (T1490)

CIS Control(s): 11.1: Establish and Maintain a Data Recovery Process, 11.4: Establish and Maintain an Isolated Instance of Recovery Data

Red Canary Atomic Red Team Test(s): T1490 - Inhibit System Recovery Atomic Test #1

Detecting the deletion of shadow copies is a great way to detect Wizard Spider preparing to encrypt your device with Ryuk.

To detect the deletion of shadow copies, write a custom rule that will alert on the execution of commands containing: "vssadmin delete shadows".

This command is commonly run in ransomware attacks as it makes restoring without paying the ransom far more difficult. By looking for unauthorized vssadmin activity, you will defend against many ransomware strains, not just Ryuk

Detection Opportunity 2: Detecting and blocking BazarLoader and BazarBackdoor C2 communications

MITRE ATT&CK: Application Layer Protocol: Web Protocols (T1071.001)

CIS Control(s): 13.3: Deploy a Network Intrusion Detection Solution (IG2+)

Red Canary Atomic Red Team Test(s): T1071.001 - Web Protocols Atomic Test #1

The Bazar family of malware uses the EmerDNS blockchain service for its DNS communications. EmerDNS is a decentralized DNS that supports the .bazar top-level domain (TLD), a defining feature of the Bazar malware family.

Setting up a blocking or alerting rule for all DNS requests to .bazar domains will greatly reduce the risk of Bazar malware from achieving communication to its C2 server

Resources

datto.com

apt.thaicert.or.th

attack.mitre.org

us-cert.cisa.gov

fireeye.com

advanced-intel.com

intezer.com

redcanary.com

blog.malwarebytes.com

blog.cobaltstrike.com

blog.chainalysis.com

ntezer.com

cert.ssi.gouv.fr

crowdstrike.com

Table of Contents

Motives

Tactics, Techniques, and Procedures

Mitigations/ Defenses

Detection Opportunities

Resources