ATT&CKing the Diamond with STIX:

Wizard Spider G0102

Michael Kaupert - Shannon Smith - Sandra Medrano - Group 30

BIT 5114 - Spring 2022

Adversary

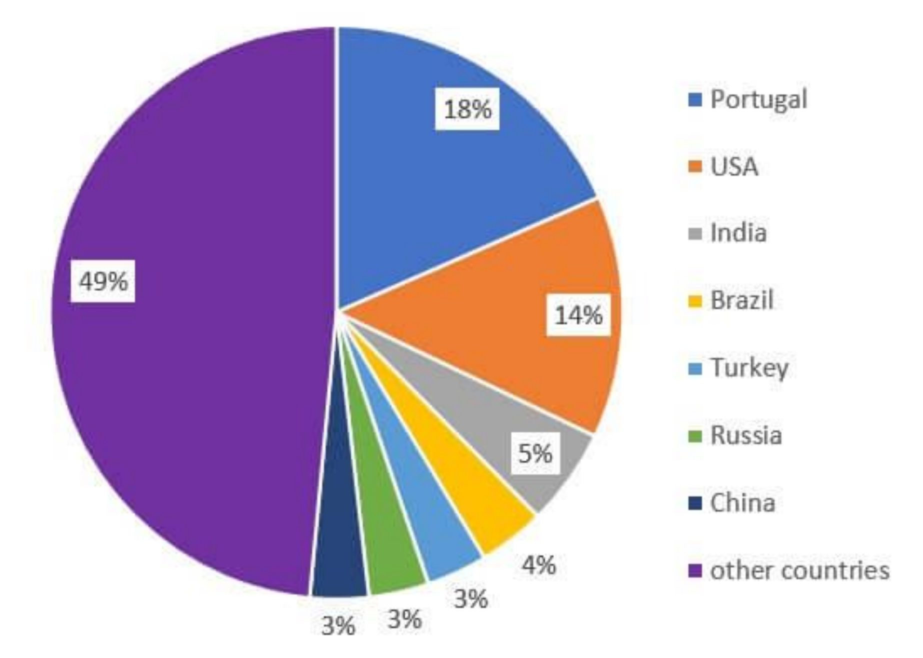
NAME:	Wizard Spider
ORIGIN:	Russia, possibly Ukraine
ALIASES:	TrickBot
DESCRIPTION:	Wizard Spider is part of the Ransom Mafia that includes other threat actors. They are a highly business-like organization, that will buy offices and hire employees.
GOALS:	They use malware tools they created to encrypt data for the purpose of ransoming it for financial gain.
SOPHISTICATION AND RESOURCE LEVEL:	Wizard Spider falls into the innovator category of the STIX model. They create their own tools, have a highly structured cyber criminal organization which funds itself from its attacks, and develops new exploits.
RELEVANT INFORMATION:	They are tolerated by the government of Russia, in some cases assist the government. Very security conscious, so they don't have a big presence on the dark web.

Victim

PERSONA(S):	Health Service Executive (Republic of Ireland), 144,000 worldwide victims in 19 nations in all industry sectors.
SECTOR(S):	Health Industry, Academic, Energy, Financial Services, Government, Manufacturing, Media, Retail, Telecommunications and Technology sectors.
ASSET(S):	Digital Assets, Email
SUSCEPTIBILITIES:	Phishing/spam, network shares, Windows Restart Manager, Lack of User Security Training
RELEVANT INFORMATION:	There are multiple victims based on each malware Wizard Spider are using at the time. In this year alone, the Trickbot malware infected 144,000 victims, however attribution is difficult. It's possible to have the victim pay ransom twice. Wizard Spider exfiltrates the data and threatens to publish it publicly or sell to competitors unless the victim pays again.

Victim

Wizard Spider victims since November 1, 2020, grouped by countries



Socio-Political

VICTIMOLOGY:	High profile victims, such as health care organizations, financial organizations, cryptocurrency exchanges, and technology firms.
INTENT OR OBJECTIVE:	Financial gain, high impact "big game hunting" ransomware attacks.
DEGREE OF PERSISTENCE:	Wizard Spider has the resources and the motivation to mount this campaign using Trickbot malware. It can install a backdoor that lets the attacker come in at will while hiding itself. It may even install other software later in order to download ransomware. This is definitely on the more enduring side of the spectrum. Later, the software can remove itself after the ransom is paid making it fleeting in that regard.
FIRST SEEN:	September 2016
LAST SEEN:	March 2022
RELEVANT INFORMATION:	TrickBot has remained a primary tool for WIZARD SPIDER and has grown to infect upward of one million systems worldwide.

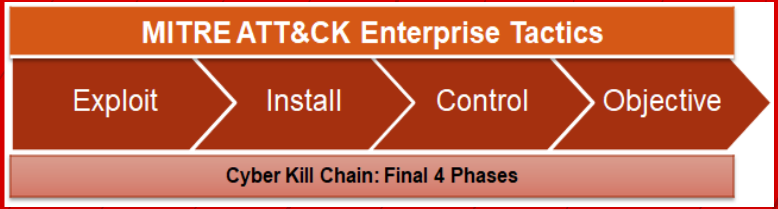
Capabilities

<table>
<tr><td><b>VULNERABILITY:</b></td><td colspan="5">TrickBot: Trojan that targets Windows machines and comes in modules accompanied by a configuration file. Each module has a specific task like gaining persistence, propagation, stealing credentials, encryption, etc. TrickBot is also capable of data exfiltration over a hardcoded C2 server, cryptomining, and host enumeration. CVE-2017-0144 and CVE-2017-0147 deal with Microsoft Windows SMBv1 and NBT Remote Code Execution. CVE-2019-0630 and CVE-2019-0633 deal with a Windows SMB Remote Code Execution Vulnerability.</td></tr>
<tr><td><b>MALWARE:</b></td><td>Trickbot
Bazar
Anchor DNS</td><td colspan="4">All fall under family of malicious Remote Access Trojans (RATs) and have been used to deploy Conti and Ryuk ransomware. Trickbot is constantly being updated with new capabilities, features and distribution vectors, enabling it to be a flexible and customizable malware that can be distributed as part of multi-purpose campaigns.</td></tr>
<tr><td><b>TOOLS:</b></td><td>Ryuk Ransomware
Conti Ransomware</td><td colspan="4">Ryuk: Variant of older Hermes ransomware; Observed since 2018, targets Microsoft Windows cybersystems.
Conti: Observed since 2020, affects all versions of Microsoft Windows.</td></tr>
<tr><td><b>RELATED IOCs:</b></td><td><b>Trickbot IOCs:</b>
After successful executable file with a 12-character randomly generated file name (e.g. mfjdieks.exe) and places this file in one of the following directories:
● C:\Windows\
● C:\Windows\SysWOW64\
● C:\Users\[Username]\AppData\Roaming\</td><td><b>Bazar IOCs:</b>
● A scheduled task named “StartAd-Ad” appears in the Windows registry with autorun entries added next
● Executable dual-extension files such as Report.DOC.exe</td><td><b>Anchor IOCs:</b>
$FILE:
● C:\Windows\SysWOW64\mntsbdyh.exe (malware-location)
$GUID:
● /anchor_dns/DESKTOP-C7FF9D5_W629200.03FCAA33763A8FE5CF0BF6FD99F5D2C/
$TASK:
● WinRAR autoupdate#83029</td><td><b>Ryuk IOCs:</b>
● Files with the file extension “.ryk”
● “RyukReadMe.txt”
● “RyukReadMe.html”</td><td><b>Conti IOCs:</b>
● Method of delivery not clear
● Implementation of AES-256 that uses up to 32 individual logical threads, making it much faster than most ransomware</td></tr>
<tr><td><b>RELEVANT INFORMATION:</b></td><td colspan="5">Wizard Spider is responsible for the core development and distribution of Trickbot, but since pivoted to downloader model.</td></tr>
</table>

Infrastructure

TYPE 1 INFRASTRUCTURE:	**PsExec:** Portable tool from Microsoft that lets you run processes remotely using another user's credentials **HTTP:** Web protocols were used for network communications **Nltest:** Windows command-line utility that was used to enumerate domain trusts **Net:** A part of the Windows operating system, that was used to obtain network information for Discovery **AdFind:** Command line active directory query tool, that was used to enumerate domain computers
TYPE 2 INFRASTRUCTURE:	**Cobalt Strike:** Commercial remote access tool, used to gain lateral movement **Empire:** An open source cross platform remote tool that is publicly available in Github and was used as a post-exploitation framework **GrimAgent:** A backdoor used for the deployment of the Ryuk ransomware. **Mimikatz:** A credential dumper tool that was used to steal AES hashes.
SERVICE PROVIDERS:	**Cloud-based services:** There has been an increase usage of leveraging cloud services to carry out malicious attacks. **Google Docs/Email:** Wizard Spider sent links through email of compromised Google drive documents and other online file hosting services
RELATED IOCs:	● Exfiltrated domain credentials and enumerated network information. ● Modification of registry keys ● Copied tools into the %TEMP% directory using stolen credentials ● Scheduled tasks under the names WinDotNeT, GoogleTask , or Sysnetsf
RELEVANT INFORMATION:	Wizard spider has a diverse set of tools within its arsenal

Technical Axis / TTPs



MITRE ATT&CK Enterprise Tactics

Cyber Kill Chain: Final 4 Phases

WIZARD SPIDER TACTICS

	Defense Evasion	Initial Access	Execution	Persistence	Privilege Escalation	Discovery
TECHNIQUES	File & Directory Permission	External Remote Services	Command & Scripting Interpreter	Boot or Logon AutoStart Execution	Process Injection	Account Discovery
	Impair Defenses	Phishing	Scheduled Task/Job	Create of Modify System Process	Registry Run Keys/Startup Folder	Network Share Discovery
	Masquerading	Valid Accounts	System Services	External Remote Services	Winlogon Helper DLL	Remote System Discovery
	Modify Registry		Windows Management Instrumentation	Valid Accounts		Software Discovery

The MITRE ATT&CK Enterprise Tactics align well with the last 4 phases of the Cyber Kill Chain

1

SOCIO-POLITICAL AXIS

VICTIMOLOGY: High-Profile

INTENT: Financial Gain

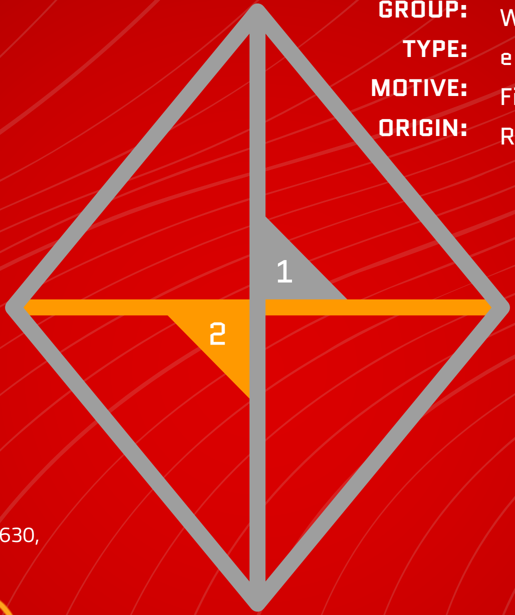
2

TECHNICAL AXIS (TTPS)

ENTERPRISE TACTICS: Defense evasion, Initial access, Escalation, Persistence, Discovery, Privilege escalation

ADVERSARY

GROUP:	Wizard Spider/Trickbot
TYPE:	eCrime
MOTIVE:	Financially Motivated
ORIGIN:	Russia, Possibly Ukraine



CAPABILITIES

MALWARE:	Trickbot, Bazar, Anchor
RANSOMWARE:	Ryuk, Conti
RELATED CVE:	CVE-2017-0144. CVE-2017-0147, CVE-2019-0630, CVE-2019- 0633

INFRASTRUCTURE

TYPE 1:	PsExec, Net,HTTP, Nltest, AdFind
TYPE 2:	Empire, GrimAgent, Cobalt Strike, Mimikatz

VICTIMS

ORGANIZATIONS:	HSE in Ireland, 144,000 victims in multiple countries, financial sector
ASSETS:	POS Machines, Networked Data, Users

References

A

Aubrey Perin, Lead. “Emotet Re-Emerges with Help from TrickBot.” *Qualys Security Blog*, 6 Jan. 2022, https://blog.qualys.com/vulnerabilities-threat-research/2022/01/06/emotet-re-emerges-with-help-from-trickbot.

C

Conti (ransomware) - Wikipedia. https://en.wikipedia.org/wiki/Conti_(ransomware). Accessed 22 Apr. 2022.

Cyber Kill Chain® | Lockheed Martin. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. Accessed 30 Apr. 2022.

D

DiMaggio, Jon. *1 RANSOM MAFIA. ANALYSIS of the WORLD’S FIRST RANSOMWARE CARTEL*. 7 Apr. 2021, analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf. Accessed 28 Apr. 2022

M

“Methods and Tactics of Advanced Persistent Threat Actor: Wizard ..”. *Youtube*, https://www.youtube.com/watch?v=a5osvPQhM5U. Accessed 20 Apr. 2022.

References

R

"Ransom Mafia. Analysis of the World's First Ransomware Cartel." *Analyst1*, analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel.

"Ransomware Activity Targeting the Healthcare and Public Health Sector | CISA." *CISA.Gov*, www.cisa.gov/uscert/ncas/alerts/aa20-302a. Accessed 28 Apr. 2022.

Reynolds, P. "'Wizard Spider': Who Are They and How Do They Operate? ". *RTE*, 19 May 2021, https://www.rte.ie/news/crime/2021/0518/1222349-ransomware-crime-group/.

RYUK Ransomware. https://www.trendmicro.com/en_us/what-is/ransomware/ryuk-ransomware.html. Accessed 27 Apr. 2022.

Ryuk (ransomware) - Wikipedia. https://en.wikipedia.org/wiki/Ryuk_(ransomware). Accessed 22 Apr. 2022.

S

"September 2021'S Most Wanted Malware: Trickbot Once Again Tops the List." *Bloomberg.com*, 8 Oct. 2021, www.bloomberg.com/press-releases/2021-10-08/september-2021-s-most-wanted-malware-trickbot-once-again-tops-the-list. Accessed 4 May 2022.

References

T

Toh, A. "Ryuk Ransomware Common Activities and IOCs | Proficio Threat Intel". *Proficio*, https://www.proficio.com/ryuk-ransomware/. Accessed 23 Apr. 2022.

"TrickBot Malware | CISA." *Www.cisa.gov*, www.cisa.gov/uscert/ncas/alerts/aa21-076a.

"TrickBot Malware Fact Sheet". *CISA.Gov*, https://us-cert.cisa.gov/sites/default/files/publications/TrickBot_Fact_Sheet_508.pdf. Accessed 28 Apr. 2022.

"Trickbot Shows Off New Trick: Password Grabber Module". *Trend Micro*, https://www.trendmicro.com/en_us/research/18/k/trickbot-shows-off-new-trick-password-grabber-module.html. Accessed 1 May 2022.

Trickbot Targets 140,000 Victims in 14 Months - Infosecurity Magazine. https://www.infosecurity-magazine.com/news/trickbot-targets-140000-victims-in/. Accessed 1 May 2022.

"Trojan.TrickBot | Malwarebytes Labs | Detections". *Malwarebytes*, https://blog.malwarebytes.com/detections/trojan-trickbot/. Accessed 23 Apr. 2022.

References

W

“What Is MITRE ATT&CK and How Is It Useful? | from Anomali.” *Www.anomali.com*, www.anomali.com/resources/what-mitre-attck-is-and-how-it-is-useful

Wizard Spider Modifies and Expands Toolset [Adversary Update]. https://www.crowdstrike.com/blog/wizard-spider-adversary-update/. Accessed 30 Apr. 2022.

“Wizard Spider, UNC1878, TEMP.MixMaster, Grim Spider, Group ..”. *MITRE*, 12 May 2020, https://attack.mitre.org/groups/G0102/.

Wizard Spider - Wikipedia. https://en.wikipedia.org/wiki/Wizard_Spider. Accessed 20 Apr. 2022.

“WIZARD SPIDER (Threat Actor)”. *Malpedia*, https://malpedia.caad.fkie.fraunhofer.de/actor/wizard_spider. Accessed 22 Apr. 2022.