datto

Table of Contents

TA551 Threat Profile

Names: TA551, Shathak, GOLD CABIN

TA551 is a cybercrime group targeting individuals and businesses globally. The group has been in operation since at least 2018 running mass email phishing campaigns in order to steal sensitive information.

Red Canary reported TA551 as the most prevalent threat actor group observed in 2020, with 15.5% of their customers affected by TA551.

Motives

TA551 is financially motivated, looking to gain access to businesses with the aim of stealing sensitive data.

Tactics, Techniques and Procedures (TTPs)

TA551's TTPs have remained relatively consistent despite utilising a range of commodity malwares in their campaigns.

TA551 spoofs legitimate email chains taken from previous victims, sending copies of the phishing email to the recipients of the original email chain. The phishing email will prompt the recipient to open the attached zip file with a provided password. This tactic gives their phishing emails a better chance of being opened as there is already an established relationship between the sender and recipient. Password protecting zipped attachments also prevents email filtering software from analyzing files inside the zip and detecting malware.

Inside the zip file is a Word document with macros. The macro will automatically download malware from actor-controlled infrastructure and establish persistence on the host.

Once persistence has been established, TA551 will download further tooling and malware to perform reconnaissance and exfiltrate sensitive data from the compromised host and network with the goal of gaining access to bank accounts.

2021-08-10: TA551 (SHATHAK) BAZARLOADER LEADS TO COBALT STRIKE

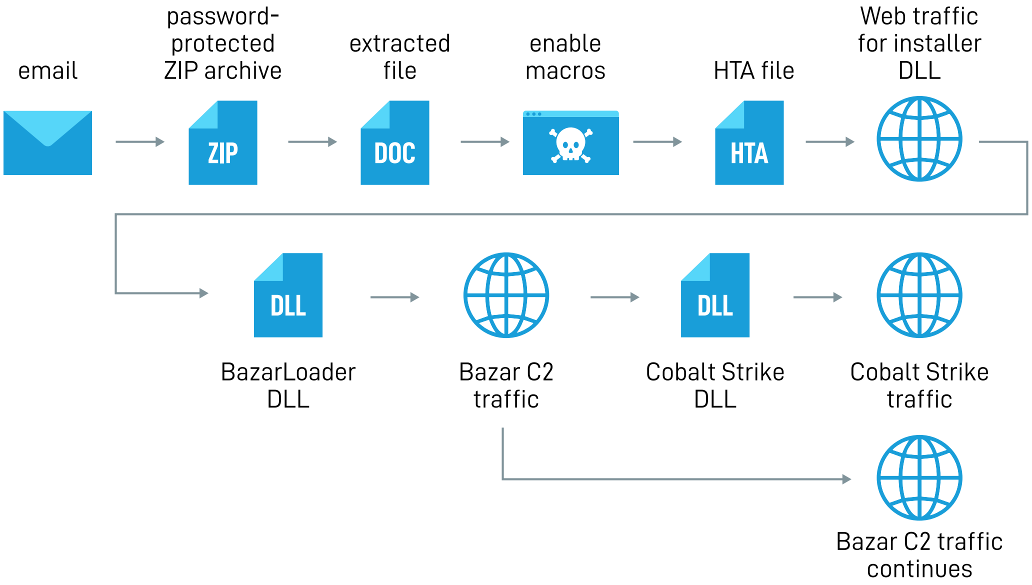


Table of Contents

MITRE ATT&CK:

The following maps TA551's TTPs to MITRE ATT&CK:

Reconnaissance	Initial Access	Execution	Defense Evasion	Command and Control
Gather Victim Identity Information	Phishing	Command and Scripting Interpreter	Masquerading	Application Layer Protocol
Email Addresses	Spearphishing Attachment	Windows Command Shell	Obfuscated Files or Information	Web Protocols
		User Execution	Steganography	Data Encoding
		Malicious File	Signed Binary Proxy Execution	Standard Encoding
			Rundll32	Dynamic Resolution
			Mshta	Domain Generation Algorithms
			Regsvr32	Ingress Tool Transfer

Reconnaissance

- **Gather Victim Identity Information: Email Addresses (T1589.002) -** TA551 has used spoofed company emails acquired from previously infected hosts to target new individuals.

Initial Access

- **Phishing: Spearphishing Attachment (T1566.001) -** TA551 has sent password-protected zip archive attachments in spearphishing emails

Table of Contents

Execution

- **Command and Scripting Interpreter: Windows Command Shell (T1059.003) -** TA551 has used the Windows command shell (cmd.exe) to execute commands
- **User Execution: Malicious File (T1204.002) -** TA551 prompts users to enable macros in their spearphishing attachments to download and install malware

Defense Evasion

- **Masquerading (T1036) -** TA551 has disguised malware DLLs as .dat and .jpg files
- **Obfuscated Files or Information: Steganography (T1027.003) -** TA551 has hidden encoded malware DLLs in a PNG
- **Signed Binary Proxy Execution: Mshta (T1218.005) -** TA551 has used mshta.exe to execute a malicious HTML Application (HTA) file.
- **Signed Binary Proxy Execution: Regsvr32 (T1218.010) -** TA551 has used regsvr32.exe to execute downloaded malicious DLLs.
- **Signed Binary Proxy Execution: Rundll32 (T1218.011) -** TA551 has used rundll32.exe to execute downloaded malicious DLLs.

Command and Control

- **Application Layer Protocol: Web Protocols (T1071.001) -** TA551 has used HTTP for Command and Control (C2) communications.
- **Data Encoding: Standard Encoding (T1132.001) -** TA551 has used encoded ASCII text for C2 communications.
- **Dynamic Resolution: Domain Generation Algorithms (T1568.002) -** TA551 has used a Domain Generation Algorithm (DGA) to generate URLs from executed macros.
- **Ingress Tool Transfer (T1105) -** TA551 has retrieved tools, installer binaries, and malware from C2.

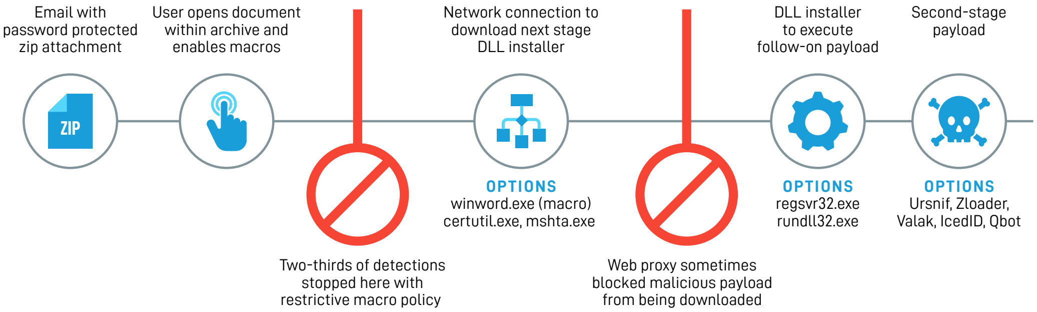
Exfiltration

- **Exfiltration Over C2 Channel (T1041) -** TA551 has used C2 channels to exfiltrate stolen data.

Mitigations/Defences

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

TA551 Intrusion Chain


Email with password protected zip attachment
ZIP
User opens document within archive and enables macros
Two-thirds of detections stopped here with restrictive macro policy
Network connection to download next stage DLL installer
OPTIONS
winword.exe (macro)
certutil.exe, mshta.exe
Web proxy sometimes blocked malicious payload from being downloaded
DLL installer to execute follow-on payload
OPTIONS
regsvr32.exe
rundll32.exe
Second-stage payload
OPTIONS
Ursnif, Zloader, Valak, IcedID, Qbot

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 TA551's MITRE ATT&CK methods to CIS v8 Safeguards:

MITRE ATT&CK	CIS Safeguards
Gather Victim Identity Information: Email Addresses (T1589.002)	None
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
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
Masquerading (T1036)	**IG1** 3.3: Configure Data Access Control Lists 4.1: Establish and Maintain a Secure Configuration Process 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process

— IG1 — IG2 — IG3

Obfuscated Files or Information: Steganography (T1027.003)	No mappings
Signed Binary Proxy Execution: Mshta (T1218.005)	**IG1** 2.3: Address Unauthorized Software 4.1: Establish and Maintain a Secure Configuration Process
Signed Binary Proxy Execution: Regsvr32 (T1218.010)	**IG2** 10.5: Enable Anti-Exploitation Features
Signed Binary Proxy Execution: Rundll32 (T1218.011)	**IG2** 10.5: Enable Anti-Exploitation Features
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
Data Encoding: Standard Encoding (T1132.001)	**IG2** 13.3: Deploy a Network Intrusion Detection Solution **IG3** 13.8: Deploy a Network Intrusion Prevention Solution
Dynamic Resolution: Domain Generation Algorithms (T1568.002)	**IG1** 9.2: Use DNS Filtering Services
Ingress Tool Transfer (T1105)	**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

— IG1 — IG2 — IG3

Detection Opportunities

While TA551's TTPs are some of the most consistent and well-known of threat actor groups, they are effective. Detecting TA551 targeting your network requires a solid understanding of their attack vectors, mapping them to actionable defensive controls, and validating your defenses through reliable, repeatable testing.

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

Detection Opportunity 1: Detecting mshta.exe execution

MITRE ATT&CK: Signed Binary Proxy Execution: Mshta (T1218.005)

CIS Control(s): 2.3: Address Unauthorized Software, 4.1: Establish and Maintain a Secure Configuration Process

Red Canary Atomic Red Team Test(s): T1218.005 - Mshta Atomic Test #3

Mshta.exe is a utility that executes Microsoft HTML Applications (HTA) files. Mshta.exe is used by TA551 to execute malicious scripts that download and install the next stage of their attack. TA551 typically launches mshta.exe from macros in Word documents. By setting up alerts for the invocation of mshta.exe from Word or Excel, you will be able to quickly discover TA551 on your network.

Parent process: winword.exe OR excel.exe

Process: mshta.exe

TA551 has been observed renaming mshta in an attempt to circumvent detections based on process name only. If possible, alerting on the execution of the process hash matching the device's legitimate copy of.

Unless you have a specific use case for Mshta.exe in your environment, Microsoft recommends blocking the application from running due to its use by attackers.

Detection Opportunity 2: Detecting malicious DLL execution

MITRE ATT&CK: Signed Binary Proxy Execution: Regsvr32 (T1218.010), Signed Binary Proxy Execution: Rundll32 (T1218.011)

CIS Control(s): 10.5: Enable Anti-Exploitation Features (IG2+)

Red Canary Atomic Red Team Test(s): T1218.010 - Regsvr32 Atomic Test #3

Once mshta.exe has reached out to the C2, it will pull down a malicious Dynamic-Link Library (DLL) file, masquerading as a different file, often a JPEG.

TA551 will then execute the file with regsvr32.exe or rundll32.exe. Regsvr32 is a built-in Windows command-line utility to register and unregister DLL files and ActiveX Control (OCX) files.

Regsvr32.exe should almost always be executing DLL or OCX files, and rundll32.exe is for DLLs only. Knowing this, writing the following alerts will help detect TA551 and other actors attempting to execute malware:

1. Alert on regsvr32.exe registering a file that doesn't have the .dll or .ocx extension
2. Alert on rundll32.exe running files that don't have the .dll extension

Resources

attack.mitre.org
redcanary.com
unit42.paloaltonetworks.com
threatresearch.ext.hp.com
success.trendmicro.com
malware-traffic-analysis.net
cisecurity.org

Table of Contents