Hive Pro

THREAT ADVISORY

Prolific threat actor TA551 using new malware IcedID	TA2022080

Threat Level	RED	Publish Date – Mar 29, 2022

TA551 is a financially motivated threat group that has been active at least since 2018. The gang primarily targeted English, German, Italian, and Japanese speakers through email-based malware distribution activities. IcedID, a modular banking trojan, is used by this threat actor to hijack current email conversation threads and inject malicious payloads.

As the first attack vector, the threat actor takes control of a critical email account in an organization in order to send a phishing email and hijack a conversation. They might be able to do so by targeting a vulnerable Microsoft Exchange server (Proxyshell or Proxylogon vulnerabilities). A ZIP file containing an ISO file would be attached to the email. A LNK and a DLL file are included in this ISO file. When the victim double-clicks the LNK file, the Regsvr32 utility runs the DLL file, which then loads the IcedID loader. The host is then scanned, and the C2 server receives the basic system information via an HTTP GET request. Then the C2 server sends a payload to the system in order to infect it.

The MITRE TTPs commonly used by IcedID are:
TA0001: Initial Access
TA0002: Execution
TA0003: Persistence
TA0004: Privilege Escalation
TA0005; Defense Evasion
TA0007: Discovery
TA0009: Collection
TA0011: Command and Control
T1087.002: Account Discovery: Domain Account
T1071.001: Application Layer Protocol: Web Protocols
T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1185: Browser Session Hijacking
T1059.005: Command and Scripting Interpreter: Visual Basic
T1573.002: Encrypted Channel: Asymmetric Cryptography
T1105: Ingress Tool Transfer
T1106: Native API
T1027: Obfuscated Files or Information
T1027.002: Software Packing
T1027.003: Steganography
T1069: Permission Groups Discovery
T1566.001: Phishing: Spearphishing Attachment
T1055.004: Process Injection: Asynchronous Procedure Call
T1053.005: Scheduled Task/Job: Scheduled Task
T1218.007: Signed Binary Proxy Execution: Msiexec
T1082: System Information Discovery
T1204.002: User Execution: Malicious File
T1047: Windows Management Instrumentation

Hive Pro

THREAT ADVISORY

Actor Details

Name	Origin	Target Locations	Target sectors	Motive
TA551 (Gold Cabin, Shathak)	Unknown	Worldwide	Energy, Financial, Healthcare, IT, Oil and gas, Telecommunications, Consumer Utilities	Financial gain

Indicators of Compromise (IoCs)

Type	Value
Domain	Yourgroceries[.]top
SHA256	3542d5179100a7644e0a747139d775dbc8d914245292209bc9038ad2413b3213, 698a0348c4bb8fffc806a1f915592b20193229568647807e88a39d2ab81cb4c2, a17e32b43f96c8db69c979865a8732f3784c7c42714197091866473bcfac8250

References

https://www.theregister.com/2022/03/29/icedid_microsoft_exchange_phishing/