Mar 27 2024

NETMANAGEIT

Intelligence Report

Threat Identification: Agent Tesla

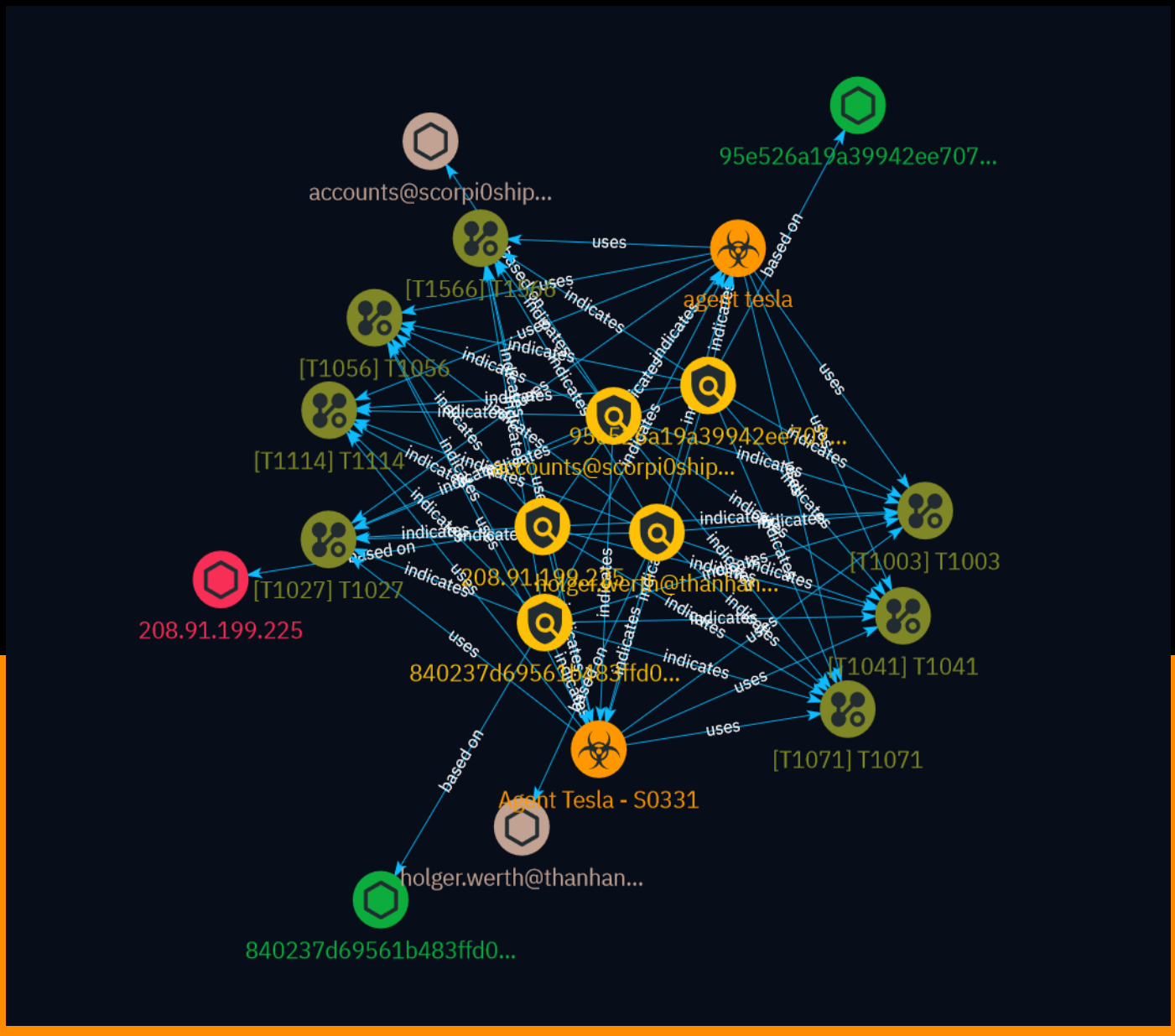

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report describes a campaign distributing Agent Tesla malware via RAR files. The malware exfiltrates system information from compromised hosts and sends it to a remote server. Technical details are provided including file hashes, C2 infrastructure, email login credentials, and network traffic patterns.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name
holger.werth@thanhancompony.com
Pattern Type
stix
Pattern
[email-addr:value = 'holger.werth@thanhancompony.com']
Name
accounts@scorpi0ship.com
Pattern Type
stix
Pattern
[email-addr:value = 'accounts@scorpi0ship.com']
Name
95e526a19a39942ee7073e28adddb685bb5bb41f889858c91bea644c657acb36

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '95e526a19a39942ee7073e28adddb685bb5bb41f889858c91bea644c657acb36']
Name
840237d69561b483ffd0905a289bde5b24a1f175b8bf7083ae2b7b1c9453663f
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '840237d69561b483ffd0905a289bde5b24a1f175b8bf7083ae2b7b1c9453663f']
Name
208.91.199.225
Pattern Type
stix
Pattern
[ipv4-addr:value = '208.91.199.225']

Malware

Name
Agent Tesla - S0331
Name
agent tesla
Description
[Agent Tesla](https://attack.mitre.org/software/S0331) is a spyware Trojan written for the .NET framework that has been observed since at least 2014.(Citation: Fortinet Agent Tesla April 2018)(Citation: Bitdefender Agent Tesla April 2020)(Citation: Malwarebytes Agent Tesla April 2020)

Attack-Pattern

Name
T1056
ID
T1056
Description
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).
Name
T1041
ID
T1041
Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Name

T1027

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

T1566

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

T1071

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and

often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

T1114

ID

T1114

Description

Adversaries may target user email to collect sensitive information. Emails may contain sensitive data, including trade secrets or personal information, that can prove valuable to adversaries. Adversaries can collect or forward email from mail servers or clients.

Name

T1003

ID

T1003

Description

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

Email-Addr

Value
holger.werth@thanhancompony.com
accounts@scorpi0ship.com

StixFile

Value
95e526a19a39942ee7073e28adddb685bb5bb41f889858c91bea644c657acb36
840237d69561b483ffd0905a289bde5b24a1f175b8bf7083ae2b7b1c9453663f

IPv4-Addr

Value
208.91.199.225

External References

- https://otx.alienvault.com/pulse/6604391c554f229c8ec4f52d