Sep 11 2023

NETMANAGEIT

Intelligence Report

Steal-It Campaign

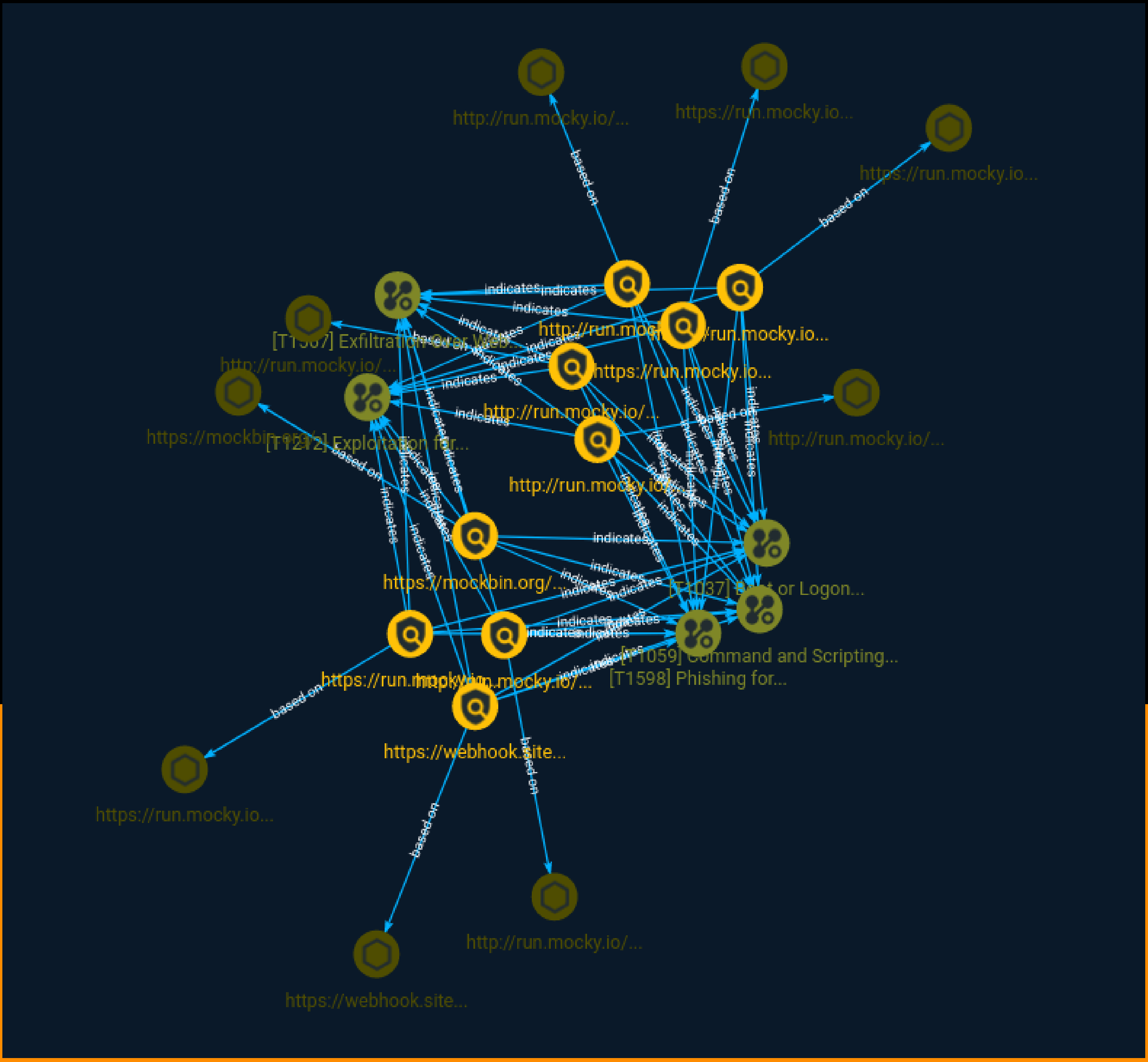

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Zscaler ThreatLabz recently discovered a new stealing campaign dubbed as the "Steal-It" campaign. In this campaign, the threat actors steal and exfiltrate NTLMv2 hashes using customized versions of Nishang's Start-CaptureServer PowerShell script, executing various system commands, and exfiltrating the retrieved data via Mockbin APIs.

Confidence

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

15 / 100

Indicator

Name

http://run.mocky.io/v3/cee6d18e-5adb-4fbd-b47b-989768473c66

Pattern Type

stix

Pattern

[url:value = 'http://run.mocky.io/v3/cee6d18e-5adb-4fbd-b47b-989768473c66']

Name

https://mockbin.org/bin/de22e2a8-d2af-4675-b70f-e42f1577da6e

Pattern Type

stix

Pattern

[url:value = 'https://mockbin.org/bin/de22e2a8-d2af-4675-b70f-e42f1577da6e']

Name

https://run.mocky.io/v3/869e530a-51f7-4bec-ae6e-3effb1737691

Pattern Type

stix

Pattern

[url:value = 'https://run.mocky.io/v3/869e530a-51f7-4bec-ae6e-3effb1737691']

Name

https://webhook.site/33128548-0eda-4e2b-bf89-7b1b225ecb9f

Pattern Type

stix

Pattern

[url:value = 'https://webhook.site/33128548-0eda-4e2b-bf89-7b1b225ecb9f']

Name

http://run.mocky.io/v3/2e757b51-c023-4bb6-9d3f-68489571abd7

Pattern Type

stix

Pattern

[url:value = 'http://run.mocky.io/v3/2e757b51-c023-4bb6-9d3f-68489571abd7']

Name

http://run.mocky.io/v3/ef2c9f34-11f5-4a99-b31c-6b203b5d5313

Pattern Type

stix

Pattern

[url:value = 'http://run.mocky.io/v3/ef2c9f34-11f5-4a99-b31c-6b203b5d5313']

Name

https://run.mocky.io/v3/f4ccbf43-9f2a-4c08-af0a-35be079694a8

Pattern Type

stix

Pattern

[url:value = 'https://run.mocky.io/v3/f4ccbf43-9f2a-4c08-af0a-35be079694a8']

Name

http://run.mocky.io/v3/99c677eb-21e1-4064-9ab4-9ee9dfd2ef13

Pattern Type

stix

Pattern

[url:value = 'http://run.mocky.io/v3/99c677eb-21e1-4064-9ab4-9ee9dfd2ef13']

Name

https://run.mocky.io/v3/e0687bb8-d14b-4ee0-8c47-202c5aaab48c

Pattern Type
stix
Pattern
[url:value = 'https://run.mocky.io/v3/e0687bb8-d14b-4ee0-8c47-202c5aaab48c']

Attack-Pattern

Name

Exploitation for Credential Access

ID

T1212

Description

Adversaries may exploit software vulnerabilities in an attempt to collect credentials. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Credentialing and authentication mechanisms may be targeted for exploitation by adversaries as a means to gain access to useful credentials or circumvent the process to gain access to systems. One example of this is MS14-068, which targets Kerberos and can be used to forge Kerberos tickets using domain user permissions.(Citation: Technet MS14-068)(Citation: ADSecurity Detecting Forged Tickets) Exploitation for credential access may also result in Privilege Escalation depending on the process targeted or credentials obtained.

Name

Boot or Logon Initialization Scripts

ID

T1037

Description

Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence. Initialization scripts can be used to perform administrative functions, which may often execute other programs or send information to an internal logging server. These scripts can vary based on operating system and whether applied locally or remotely. Adversaries may use these scripts to maintain persistence on a single system. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary. An adversary may also be able to escalate their privileges since some boot or logon initialization scripts run with higher privileges.

Name

Phishing for Information

ID

T1598

Description

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from [Phishing](https://attack.mitre.org/techniques/T1566) in that the objective is gathering data from the victim rather than executing malicious code. 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 credential harvesting campaigns. Adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means.(Citation: ThreatPost Social Media Phishing)(Citation: TrendMictro Phishing)(Citation: PCMag FakeLogin)(Citation: Sophos Attachment)(Citation: GitHub Phishery) Victims may also receive phishing messages that direct them to call a phone number where the adversary attempts to collect confidential information.(Citation: Avertium callback phishing) Phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages. 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) Phishing for information may also involve 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)

Name

Exfiltration Over Web Service

ID

T1567

Description

Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services. Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Url

Value
https://webhook.site/33128548-0eda-4e2b-bf89-7b1b225ecb9f
https://mockbin.org/bin/de22e2a8-d2af-4675-b70f-e42f1577da6e
https://run.mocky.io/v3/869e530a-51f7-4bec-ae6e-3effb1737691
https://run.mocky.io/v3/f4ccbf43-9f2a-4c08-af0a-35be079694a8
https://run.mocky.io/v3/e0687bb8-d14b-4ee0-8c47-202c5aaab48c
http://run.mocky.io/v3/cee6d18e-5adb-4fbd-b47b-989768473c66
http://run.mocky.io/v3/ef2c9f34-11f5-4a99-b31c-6b203b5d5313
http://run.mocky.io/v3/2e757b51-c023-4bb6-9d3f-68489571abd7
http://run.mocky.io/v3/99c677eb-21e1-4064-9ab4-9ee9dfd2ef13

External References

- https://otx.alienvault.com/pulse/64ff232c2e4a8d48955820a5
- https://www.zscaler.com/blogs/security-research/steal-it-campaign