Mar 01 2024

NETMANAGEIT

Intelligence Report

Don't get BITTER about being targeted -- fight back with the help of the community.

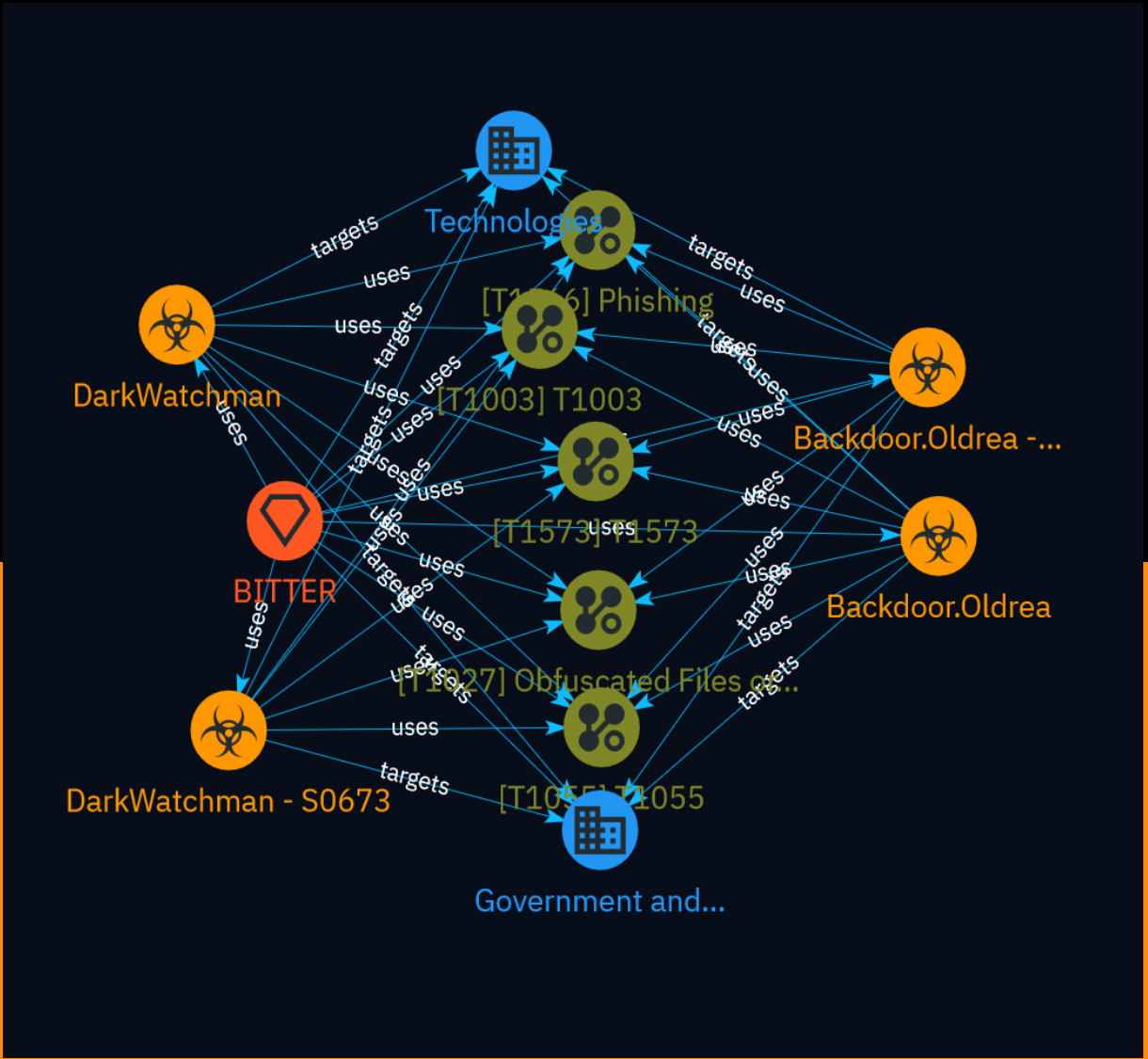

Table of contents

Overview

Entities

External References

Overview

Description

When enterprise security operations centers receive alerts about obvious true positive detections, they want to quickly understand the severity to determine if it is a critical threat that needs immediate containment. Threat intelligence analysts can provide context about whether the attack is part of a bigger campaign. Although some victim and vendor analysis is still closely held, there has been a clear increase in sharing of threat intelligence within the TLP-white community. Analysts often cannot submit samples to services like VirusTotal due to privacy restrictions, so they cannot take advantage of crowdsourced threat intel. The CARA platform guides analysts through investigative steps without compromising controls. By pivoting on domains, behaviors and code similarities, analysts can connect alerts to related attacks, like BITTER campaigns, to inform response priorities.

Confidence

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

100 / 100

Content

N/A

Malware

Name
Backdoor.Oldrea - S0093

Name
DarkWatchman - S0673

Name
DarkWatchman

Description
[DarkWatchman](https://attack.mitre.org/software/S0673) is a lightweight JavaScript-based remote access tool (RAT) that avoids file operations; it was first observed in November 2021.(Citation: Prevailion DarkWatchman 2021)

Name
Backdoor.Oldrea

Description
[Backdoor.Oldrea](https://attack.mitre.org/software/S0093) is a modular backdoor that used by [Dragonfly](https://attack.mitre.org/groups/G0035) against energy companies since at least 2013. [Backdoor.Oldrea](https://attack.mitre.org/software/S0093) was distributed via supply chain compromise, and included specialized modules to enumerate

and map ICS-specific systems, processes, and protocols.(Citation: Symantec Dragonfly) (Citation: Gigamon Berserk Bear October 2021)(Citation: Symantec Dragonfly Sept 2017)

Intrusion-Set

Name
BITTER

Description
[BITTER](https://attack.mitre.org/groups/G1002) is a suspected South Asian cyber espionage threat group that has been active since at least 2013. [BITTER](https://attack.mitre.org/groups/G1002) has primarily targeted government, energy, and engineering organizations in Pakistan, China, Bangladesh, and Saudi Arabia.(Citation: Cisco Talos Bitter Bangladesh May 2022)(Citation: Forcepoint BITTER Pakistan Oct 2016)

Attack-Pattern

Name
T1573
ID
T1573
Description
Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.
Name
Obfuscated Files or Information
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

Phishing

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

T1055

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

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.

Sector

Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.
Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

External References

- https://blog.strikeready.com/blog/dont-get-bitter-about-being-targeted--fight-back-with-the-help-of-the-community./
- https://otx.alienvault.com/pulse/65e204b10e92606d03bfd93b