Jun 27 2024

NETMANAGEIT

Intelligence Report

GrimResource - Microsoft Management Console for initial access and evasion

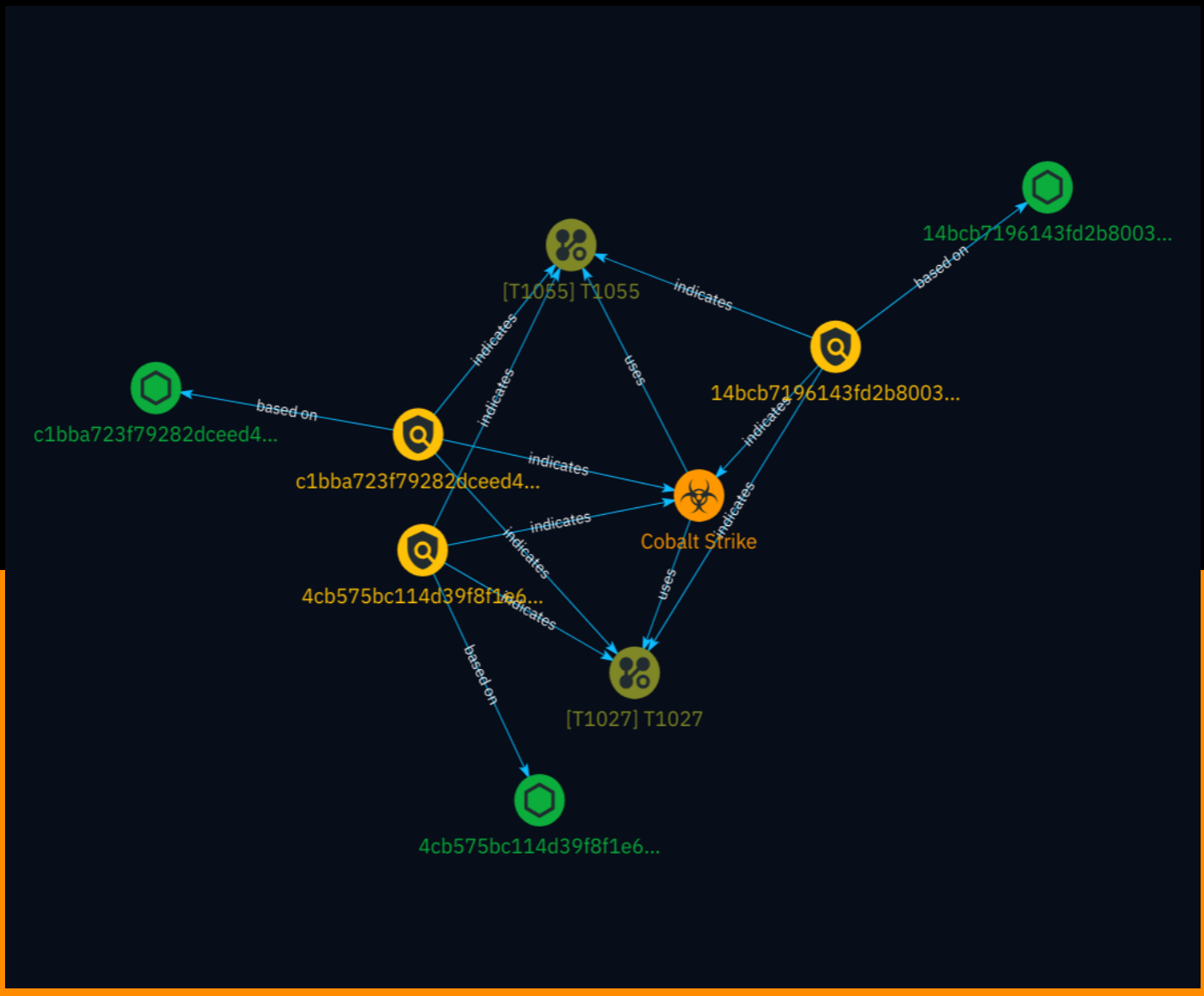

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A novel, in-the-wild code execution technique leveraging Microsoft Management Console files (MSC) has been identified by Elastic Security researchers and was first spotted in the wild in June 2016 and is currently being investigated by VirusTotal.

Confidence

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

100 / 100

Content

N/A

Attack-Pattern

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
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)

Indicator

Name

14bcb7196143fd2b800385e9b32cfacd837007b0face71a73b546b53310258bb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '14bcb7196143fd2b800385e9b32cfacd837007b0face71a73b546b53310258bb']

Name

4cb575bc114d39f8f1e66d6e7c453987639289a28cd83a7d802744cd99087fd7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4cb575bc114d39f8f1e66d6e7c453987639289a28cd83a7d802744cd99087fd7']

Name

c1bba723f79282dceed4b8c40123c72a5dfcf4e3ff7dd48db8cb6c8772b60b88

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c1bba723f79282dceed4b8c40123c72a5dfcf4e3ff7dd48db8cb6c8772b60b88']

Malware

Name
Cobalt Strike

Description
[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

based-on

Name
Name
Name

indicates

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

uses

Name

Description
[Cobalt Strike](https://attack.mitre.org/software/S0154) can hash functions to obfuscate calls to the Windows API and use a public/private key pair to encrypt Beacon session metadata.(Citation: Talos Cobalt Strike September 2020)(Citation: Cobalt Strike Manual 4.3 November 2020)

Name

Description
[Cobalt Strike](https://attack.mitre.org/software/S0154) can inject a variety of payloads into processes dynamically chosen by the adversary.(Citation: cobaltstrike manual) (Citation: Cobalt Strike Manual 4.3 November 2020)(Citation: DFIR Conti Bazar Nov 2021)

StixFile

Value
c1bba723f79282dceed4b8c40123c72a5dfcf4e3ff7dd48db8cb6c8772b60b88
14bcb7196143fd2b800385e9b32cfacd837007b0face71a73b546b53310258bb
4cb575bc114d39f8f1e66d6e7c453987639289a28cd83a7d802744cd99087fd7

External References

- https://www.elastic.co/security-labs/grimresource
- https://otx.alienvault.com/pulse/667d9b3db0a27398841a0900