Mar 06 2024

NETMANAGEIT

Intelligence Report

It'll be back: Attackers still abusing Terminator tool and variants

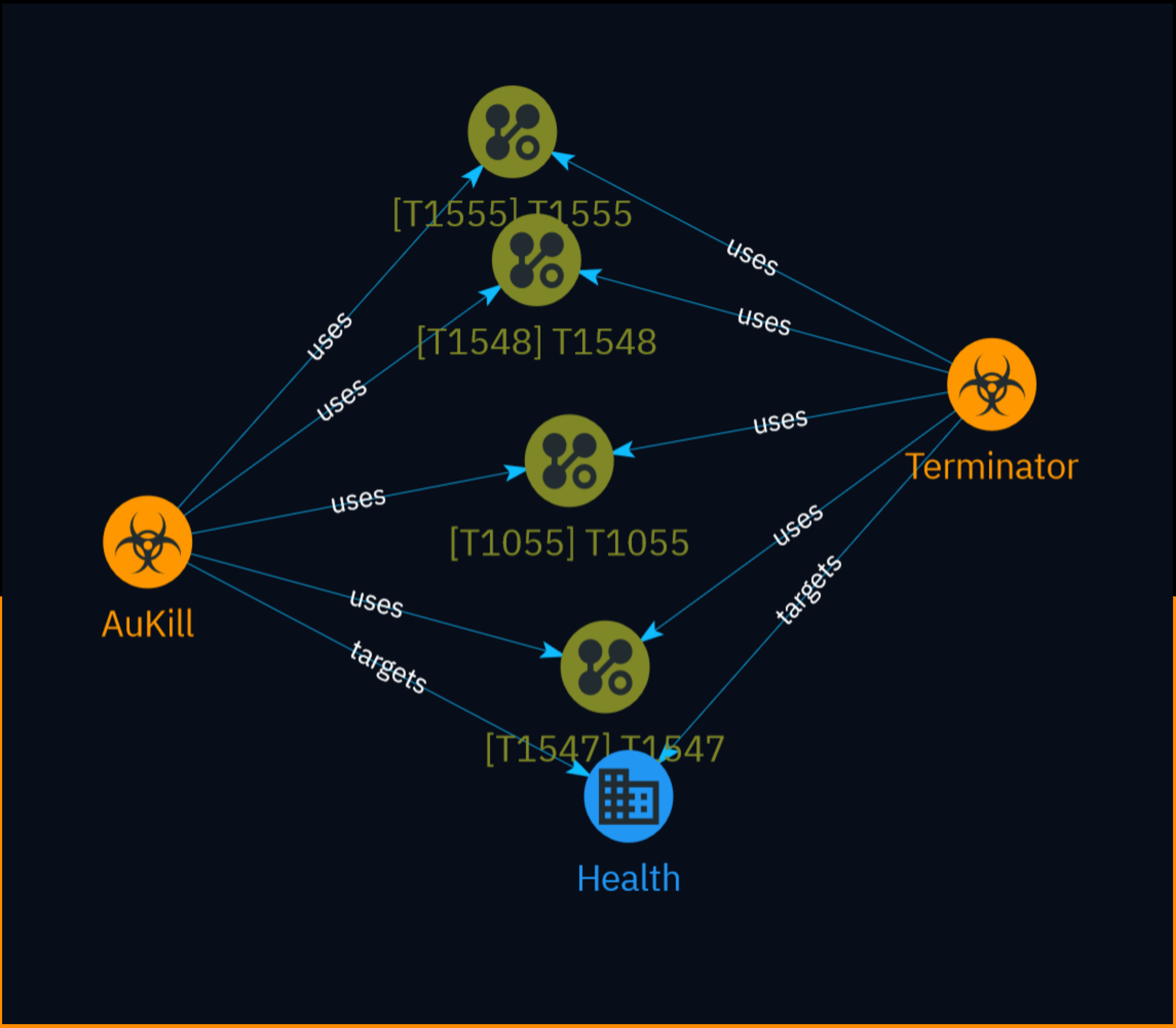

Table of contents

Overview

Entities

External References

Overview

Description

A threat intelligence report describes that threat actors continue to leverage vulnerable drivers like Zemana Anti-Logger and Anti-Malware to disable security products through Bring Your Own Vulnerable Driver attacks. Variants of the Terminator tool that exploits these drivers are still observed in the wild. The actors use the drivers for lateral movement and privilege escalation as part of ransomware campaigns targeting healthcare and other industries.

Confidence

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

100 / 100

Content

N/A

Malware

Name
AuKill

Name
Terminator

Attack-Pattern

Name

T1548

ID

T1548

Description

Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.

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
T1555

ID
T1555

Description
Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Name
T1547

ID
T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

Sector

Name
Health
Description
Public and private entities involved in research, services and manufacturing activities related to public health.

External References

- https://github.com/sophoslabs/IoCs/blob/master/Zemana-driver-IoCs.csv
- https://news.sophos.com/en-us/2024/03/04/itll-be-back-attackers-still-abusing-terminator-tool-and-variants/
- https://otx.alienvault.com/pulse/65e88af176d9bcf414357b0e