Jul 24 2023

NETMANAGEIT

Intelligence Report

First-ever Open-Source Software Supply Chain Attacks

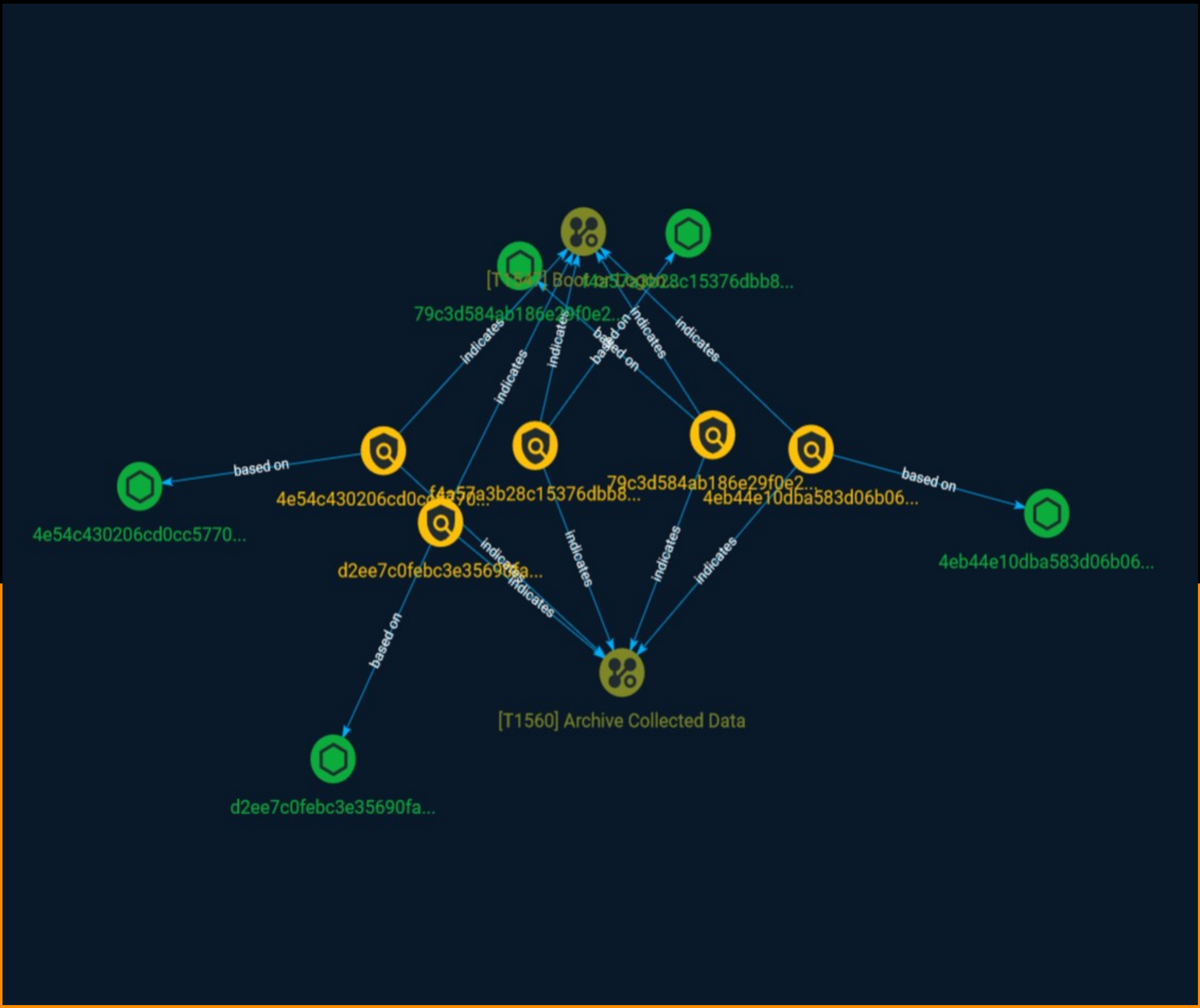

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Two separate open-source software supply-chain attacks targeting the banking sector have been identified by researchers.

Confidence

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

15 / 100

Indicator

Name
79c3d584ab186e29f0e20a67187ba132098d01c501515cfdef4265bbbd8cbcbf
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '79c3d584ab186e29f0e20a67187ba132098d01c501515cfdef4265bbbd8cbcbf']
Name
4e54c430206cd0cc57702ddbf980102b77da1c2f8d6d345093819d24c875e91a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4e54c430206cd0cc57702ddbf980102b77da1c2f8d6d345093819d24c875e91a']
Name

d2ee7c0febc3e35690fa2840eb707e1c9f8a125fe515cc86a43ba485f5e716a7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'd2ee7c0febc3e35690fa2840eb707e1c9f8a125fe515cc86a43ba485f5e716a7']

Name

4eb44e10dba583d06b060abe9f611499eee8eec8ca5b6d007ed9af40df87836d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'4eb44e10dba583d06b060abe9f611499eee8eec8ca5b6d007ed9af40df87836d']

Name

f4a57a3b28c15376dbb8f6b4d68c8cb28e6ba9703027ac66cbb76ee0eb1cd0c9

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'f4a57a3b28c15376dbb8f6b4d68c8cb28e6ba9703027ac66cbb76ee0eb1cd0c9']
```

Attack-Pattern

Name

Boot or Logon Autostart Execution

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.

Name

Archive Collected Data

ID

T1560

Description

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

StixFile

Value
f4a57a3b28c15376dbb8f6b4d68c8cb28e6ba9703027ac66cbb76ee0eb1cd0c9
d2ee7c0febc3e35690fa2840eb707e1c9f8a125fe515cc86a43ba485f5e716a7
79c3d584ab186e29f0e20a67187ba132098d01c501515cfdef4265bbbd8cbcbf
4eb44e10dba583d06b060abe9f611499eee8eec8ca5b6d007ed9af40df87836d
4e54c430206cd0cc57702ddbf980102b77da1c2f8d6d345093819d24c875e91a

External References

- https://otx.alienvault.com/pulse/64be768dce240304bdaf6597
- https://cybersecuritynews.com/first-ever-open-source-supply-chain-attack/