Sep 16 2023

NETMANAGEIT

Intelligence Report

RedLine/Vidar Abuses EV Certificates, Shifts to Ransomware

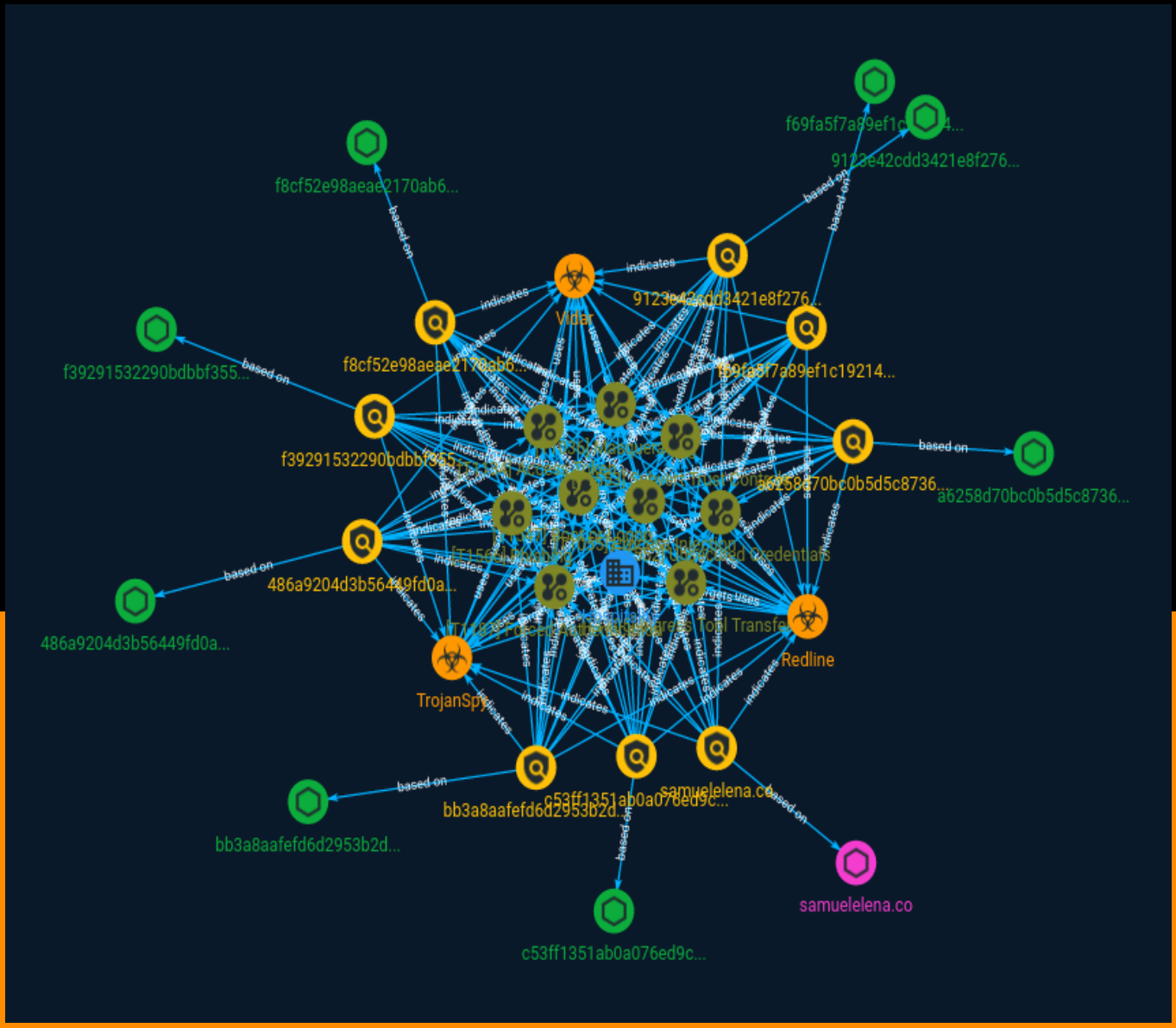

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Trend Micro investigation shows that the threat actors behind RedLine and Vidar now distribute ransomware payloads with the same delivery techniques they use to spread info stealers.

Confidence

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

15 / 100

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
Forced Authentication
ID
T1187

Description

Adversaries may gather credential material by invoking or forcing a user to automatically provide authentication information through a mechanism in which they can intercept. The Server Message Block (SMB) protocol is commonly used in Windows networks for authentication and communication between systems for access to resources and file sharing. When a Windows system attempts to connect to an SMB resource it will automatically attempt to authenticate and send credential information for the current user to the remote system. (Citation: Wikipedia Server Message Block) This behavior is typical in enterprise environments so that users do not need to enter credentials to access network resources. Web Distributed Authoring and Versioning (WebDAV) is also typically used by Windows systems as a backup protocol when SMB is blocked or fails. WebDAV is an extension of HTTP and will typically operate over TCP ports 80 and 443. (Citation: Didier Stevens WebDAV Traffic) (Citation: Microsoft Managing WebDAV Security) Adversaries may take advantage of this behavior to gain access to user account hashes through forced SMB/WebDAV authentication. An adversary can send an attachment to a user through spearphishing that contains a resource link to an external server controlled by the adversary (i.e. [Template Injection](https://attack.mitre.org/techniques/T1221)), or place a specially crafted file on navigation path for privileged accounts (e.g. .SCF file placed on desktop) or on a publicly accessible share to be accessed by victim(s). When the user's system accesses the untrusted resource it will attempt authentication and send information, including the user's hashed credentials, over SMB to the adversary controlled server. (Citation: GitHub Hashjacking) With access to the credential hash, an adversary can perform off-line [Brute Force](https://attack.mitre.org/techniques/T1110) cracking to gain access to plaintext credentials. (Citation: Cylance Redirect to SMB) There are several different ways this can occur. (Citation: Osanda Stealing NetNTLM Hashes) Some specifics from in-the-wild use include: * A spearphishing attachment containing a document with a resource that is automatically loaded when the document is opened (i.e. [Template Injection](https://attack.mitre.org/techniques/T1221)). The document can include, for example, a request similar to `file[:]//[remote address]/Normal.dotm` to trigger the SMB request. (Citation: US-CERT APT Energy Oct 2017) * A modified .LNK or .SCF file with the icon filename pointing to an external reference such as `\\[remote address]\pic.png` that will force the system to load the resource when the icon is rendered to repeatedly gather credentials. (Citation: US-CERT APT Energy Oct 2017)

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

Name

Process Injection

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

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

Subvert Trust Controls

ID

T1553

Description

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security

products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

Name

Ingress Tool Transfer

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas)

Name

Access Token Manipulation

ID

T1134

Description

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001)) or used to spawn a new process (i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.(Citation: Pentestlab Token Manipulation) Any standard user can use the `runas` command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

Name

Unsecured Credentials

ID

T1552

Description

Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g. [Bash History](https://attack.mitre.org/techniques/T1552/003)), operating system or application-specific repositories (e.g. [Credentials in Registry](https://attack.mitre.org/techniques/T1552/002)), or other specialized files/artifacts (e.g. [Private Keys](https://attack.mitre.org/techniques/T1552/004)).

Sector

Name
Hospitality
Description
Private entities offering to customers' leisure activities and experiences.

Indicator

Name
486a9204d3b56449fd0af14bba165fd36182846a9cd9b17837d0f4f818de09e4
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '486a9204d3b56449fd0af14bba165fd36182846a9cd9b17837d0f4f818de09e4']
Name
f69fa5f7a89ef1c19214ee0c8db393ced2b166bc2f7876e3b09e7903b46d21d0
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f69fa5f7a89ef1c19214ee0c8db393ced2b166bc2f7876e3b09e7903b46d21d0']
Name

c53ff1351ab0a076ed9c5868e42627939739cfaa98786a111884a3a4dd829747

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c53ff1351ab0a076ed9c5868e42627939739cfaa98786a111884a3a4dd829747']

Name

f8cf52e98aeae2170ab68d53b99b104fa6320f54057a63d2603ecdb2ec559fc1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f8cf52e98aeae2170ab68d53b99b104fa6320f54057a63d2603ecdb2ec559fc1']

Name

a6258d70bc0b5d5c87368c5024d3f23585790b14227b8c59333413082524a956

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a6258d70bc0b5d5c87368c5024d3f23585790b14227b8c59333413082524a956']

Name

bb3a8aafefd6d2953b2de555a085474fad6ba3b43eb60f0d594adac08b9d9cc3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bb3a8aafefd6d2953b2de555a085474fad6ba3b43eb60f0d594adac08b9d9cc3']

Name

9123e42cdd3421e8f276ac711988fb8a8929172fa76674ec4de230e6d528d09a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9123e42cdd3421e8f276ac711988fb8a8929172fa76674ec4de230e6d528d09a']

Name

samuelelena.co

Pattern Type

stix

Pattern

[domain-name:value = 'samuelelena.co']

Name

f39291532290bdbbf355e79bb67019225622da9699adb5fd66cbb408cee99835

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f39291532290bdbbf355e79bb67019225622da9699adb5fd66cbb408cee99835']

Malware

Name
Vidar

Name
Redline

Name
TrojanSpy

Domain-Name

Value
samuelelena.co

StixFile

Value
486a9204d3b56449fd0af14bba165fd36182846a9cd9b17837d0f4f818de09e4
bb3a8aafefd6d2953b2de555a085474fad6ba3b43eb60f0d594adac08b9d9cc3
a6258d70bc0b5d5c87368c5024d3f23585790b14227b8c59333413082524a956
f8cf52e98aeae2170ab68d53b99b104fa6320f54057a63d2603ecdb2ec559fc1
c53ff1351ab0a076ed9c5868e42627939739cfaa98786a111884a3a4dd829747
f39291532290bdbbf355e79bb67019225622da9699adb5fd66cbb408cee99835
f69fa5f7a89ef1c19214ee0c8db393ced2b166bc2f7876e3b09e7903b46d21d0
9123e42cdd3421e8f276ac711988fb8a8929172fa76674ec4de230e6d528d09a

External References

- https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/i/redline-vidar-first-abuses-ev-certificates-then-shifts-to-ransomware-/IOCs-RedLineVidar-Abuses-EV%20Certificates-Shifts-to-Ransomware.txt
- https://otx.alienvault.com/pulse/6504b35ae9b94dce7a67ff63
- https://www.trendmicro.com/en_us/research/23/i/redline-vidar-first-abuses-ev-certificates.html