Jun 19 2024

NETMANAGEIT

Intelligence Report

SolarMarker Impersonates Job Employment Website

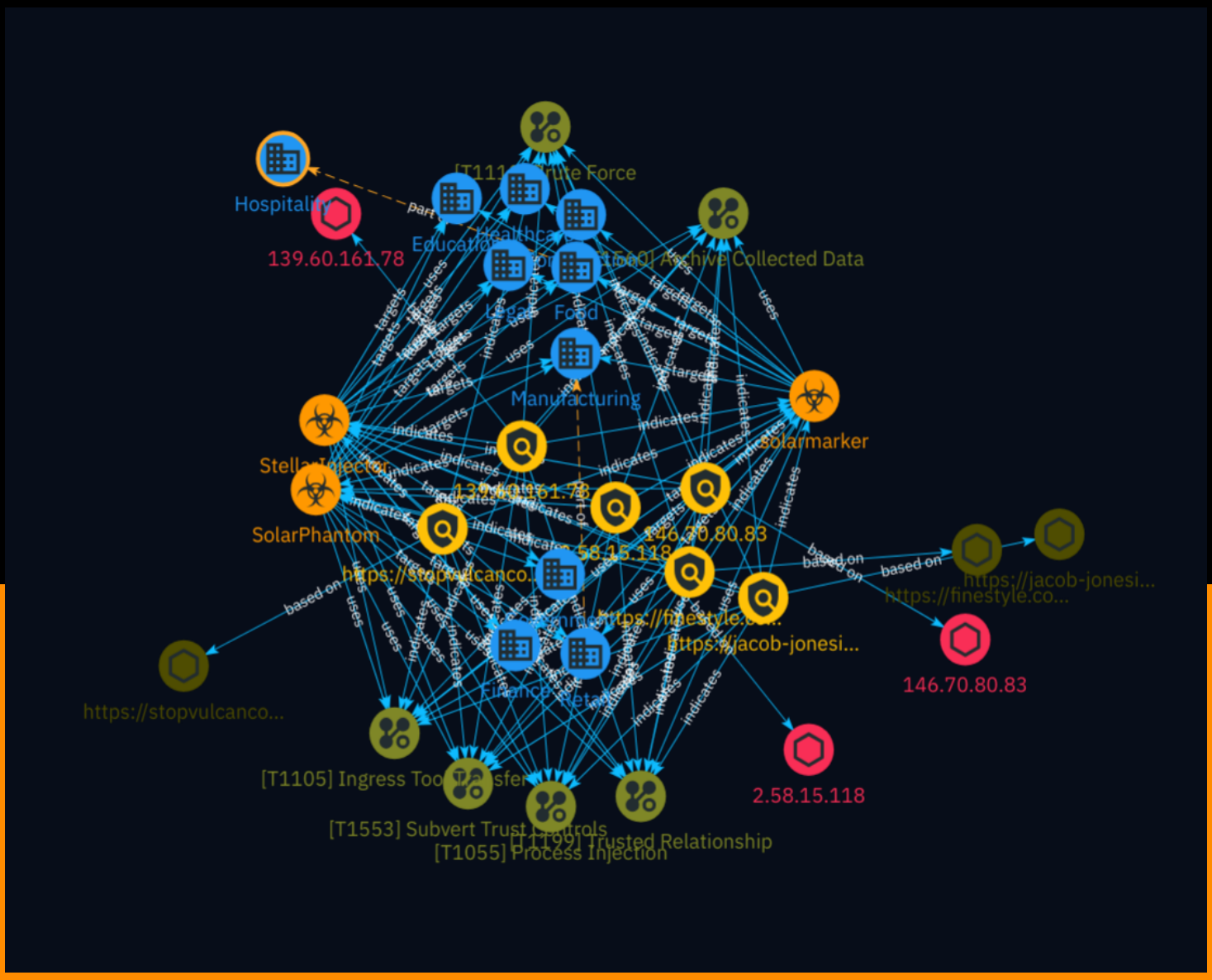

Table of contents

Overview

Entities

Observables

External References

Overview

Description

On April 2024, Cyber Analysts responded to a SolarMarker infection event. The infection occurred through a drive-by download when a user, while searching for workplace team-building ideas on Bing, was directed to a malicious site impersonating the global employment website, Indeed.

Confidence

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

100 / 100

Content

N/A

Attack-Pattern

Name

Brute Force

ID

T1110

Description

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained.(Citation: TrendMicro Pawn Storm Dec 2020) Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism.(Citation: Dragos Crashoverride 2018) Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery] (https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

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

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

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.(Citation: DOJ GRU Indictment Jul 2018) 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.

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)). 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) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Adversaries have also abused file application features, such as the Windows `search-ms` protocol handler, to deliver malicious files to victims through remote file searches invoked by [User Execution](https://attack.mitre.org/techniques/T1204) (typically after interacting with [Phishing](https://attack.mitre.org/techniques/T1566) lures).(Citation: T1105: Trellix_search-ms) 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) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

Trusted Relationship

ID

T1199

Description

Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship abuses an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network. Organizations often grant elevated access to second or third-party external providers in order to allow them to manage internal systems as well as cloud-based environments. Some examples of these relationships include IT services contractors, managed security providers, infrastructure contractors (e.g. HVAC, elevators, physical security). The third-party provider's access may be intended to be limited to the infrastructure being maintained, but may exist on the same network as the rest of the enterprise. As such, [Valid Accounts](https://attack.mitre.org/techniques/T1078) used by the other party for access to internal network systems may be compromised and used. (Citation: CISA IT Service Providers) In Office 365 environments, organizations may grant

Microsoft partners or resellers delegated administrator permissions. By compromising a partner or reseller account, an adversary may be able to leverage existing delegated administrator relationships or send new delegated administrator offers to clients in order to gain administrative control over the victim tenant.(Citation: Office 365 Delegated Administration)

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.
Name
Education
Name
Legal
Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.
Name

Hospitality

Description

Private entities offering to customers' leisure activities and experiences.

Name

Retail

Description

Distribution and sale of goods directly to the consumer.

Name

Construction

Name

Food

Description

Businesses preparing and serving food and drinks to customers in exchange for money.

Name

Healthcare

Description

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

Name
Government
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Indicator

Name
https://jacob-jonesinvestigation.com
Pattern Type
stix
Pattern
[url:value = 'https://jacob-jonesinvestigation.com']
Name
146.70.80.83
Description
CC=DK ASN=AS9009 M247 Europe SRL
Pattern Type
stix
Pattern
[ipv4-addr:value = '146.70.80.83']

Name

https://stopvulcancomalcounty.info

Pattern Type

stix

Pattern

[url:value = 'https://stopvulcancomalcounty.info']

Name

2.58.15.118

Description

ISP: GWY IT PTY LTD **OS:** Linux ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u3 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCl7wmjKwI5HFtF1DpPdBWf1qxupwPH5RSfdTGydffeBWCa udFYnopkWHg29E0KbyIQpfA2lkFxbgBJad7N+d3bFnYRnTGQ+fUpRyrHYK+17V6IS9J38R533xoDTQq0PlgWs8UQHwGstehzaz9NuEmixu4IzTglx6PmvU4Gvboqr5O24fnK4cRn2eWF1Av+tKNWdBkU 9j0ViDyhwg/ BolTWBMa+66tkp9fiF8QM0WFRsHwV7M4V3ElF+r5yefT6CMkI3KLM88CMjVGjsKeA DBsqiLs1HHhMTrfK4P7MnGHi85ZxrF0Kp9/4G6KiOaP7dR8/xFdynFpVZJPvCBm9eSyX/8RXJAZZ LgdNBzw04DON7bRW+QcsIgS+oHl2sQsdV8prdC98gbcryiCHk9YHEOW+s3TCP/ wpJc5bMdTQTCE3 1qrhYc7qmsi5V1B2w1RhEFS5/EC+N+fU9Q2RXm4K4F2R+3Q2UCVQ4xj/ wUGA5ADqH14YI6hxfYTv PbmcfDzMP0M= Fingerprint: 44:78:cd:80:1d:12:81:b3:b3:47:02:36:88:75:ad:47 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression

Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 404 NOT FOUND Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: keep-alive ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '2.58.15.118']

Name

139.60.161.78

Description

ISP: HOSTKEY **OS:** - ---------- Services: **55000:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.7 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLRT7QtljehhM44lPHxnQsQThNWSMP8eFLLOznE4heWPuscePQJPmCiE2MP+k2HmMaMjURS/g5qXrMrhU1ZkBdk= Fingerprint: cd:e7:ea:d9:83:ad:d1:bb:fa:24:f4:eb:ee:cf:68:3e Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern
[ipv4-addr:value = '139.60.161.78']
Name
https://finestyle.com/
Pattern Type
stix
Pattern
[url:value = 'https://finestyle.com/']

Malware

Name
solarmarker

Name
SolarPhantom

Name
StellarInjector

indicates

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name
Name
Name

uses

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name

targets

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

part-of

Name

Description
Sector Food and drinks businesses is a subsector of Hospitality

based-on

Name
Name
Name

IPv4-Addr

Value
139.60.161.78
2.58.15.118
146.70.80.83

External References

- https://www.esentire.com/blog/solarmarker-impersonates-job-employment-website-indeed-with-a-team-building-themed-lure
- https://otx.alienvault.com/pulse/66720016effeee5a8a1140e9