Jun 19 2023

NETMANAGEIT

Intelligence Report

Lazarus Threat Group Exploiting Vulnerability of Korean Finance Security Solution

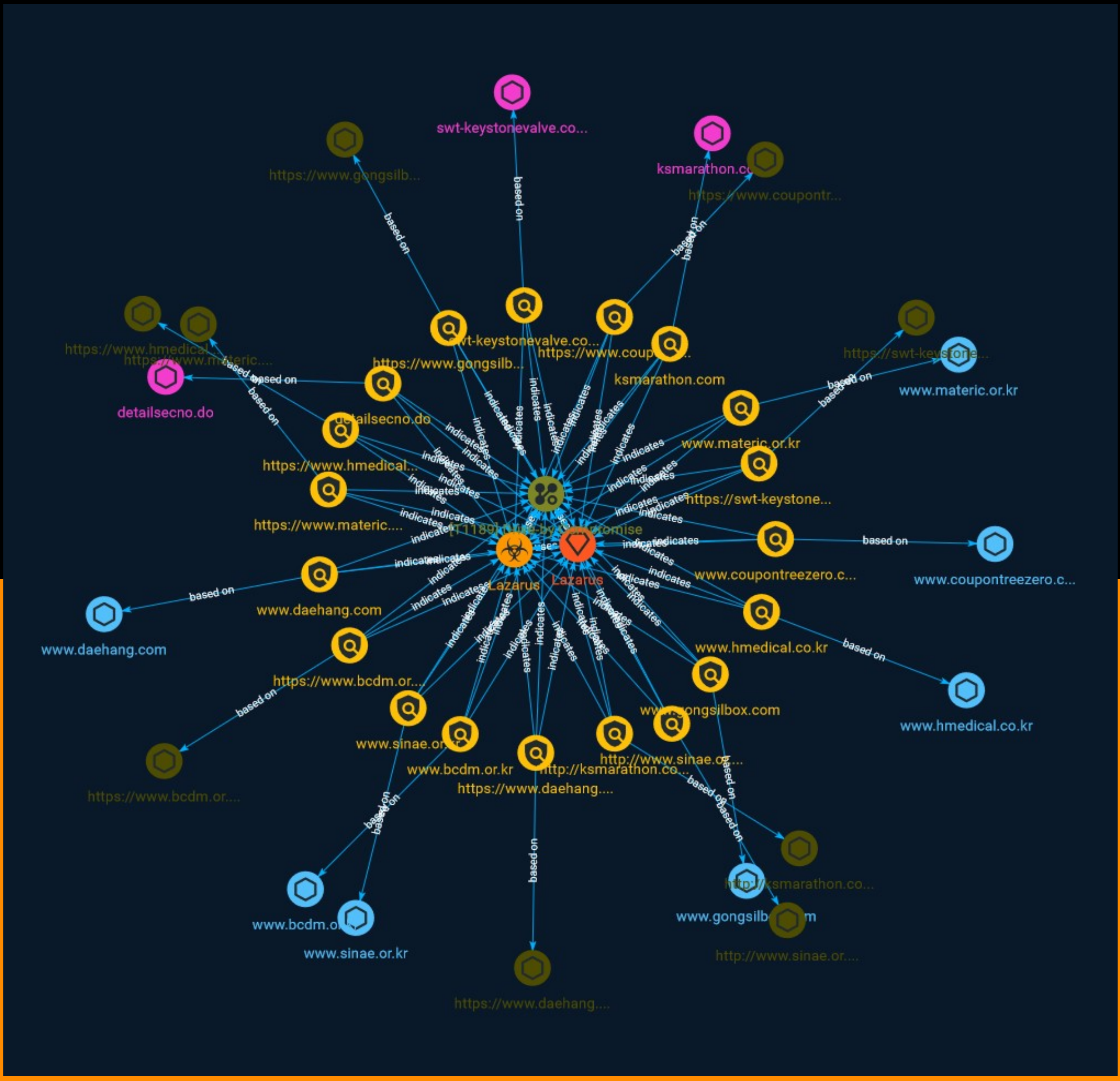

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers have identified a zero-day vulnerability in two of the financial security solutions used by companies in Korea, which have been targeted by the Lazarus threat group.

Confidence

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

15 / 100

Attack-Pattern

Name
Drive-by Compromise
ID
T1189
Description
Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable

version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

Indicator

Name
http://www.sinae.or.kr/sub01/index.asp
Pattern Type
stix
Pattern
[url:value = 'http://www.sinae.or.kr/sub01/index.asp']
Name
https://www.materic.or.kr/files/board/equip/equip_ok.asp
Pattern Type
stix
Pattern
[url:value = 'https://www.materic.or.kr/files/board/equip/equip_ok.asp']
Name
www.materic.or.kr

Pattern Type

stix

Pattern

[hostname:value = 'www.materic.or.kr']

Name

www.bcdm.or.kr

Pattern Type

stix

Pattern

[hostname:value = 'www.bcdm.or.kr']

Name

https://www.gongsilbox.com/board/bbs.asp

Pattern Type

stix

Pattern

[url:value = 'https://www.gongsilbox.com/board/bbs.asp']

Name

www.hmedical.co.kr

Pattern Type

stix

Pattern

[hostname:value = 'www.hmedical.co.kr']

Name

https://www.bcdm.or.kr/board/type3_D/edit.asp

Pattern Type

stix

Pattern

[url:value = 'https://www.bcdm.or.kr/board/type3_D/edit.asp']

Name

https://www.coupontreezero.com/include/bottom.asp

Pattern Type

stix

Pattern

[url:value = 'https://www.coupontreezero.com/include/bottom.asp']

Name

https://www.daehang.com/member/logout.asp

Pattern Type

stix

Pattern

[url:value = 'https://www.daehang.com/member/logout.asp']

Name

https://www.hmedical.co.kr/include/edit.php

Pattern Type

stix

Pattern

[url:value = 'https://www.hmedical.co.kr/include/edit.php']

Name

https://swt-keystonevalve.com/data/content/cache/cache.php?mode=read

Pattern Type

stix

Pattern

[url:value = 'https://swt-keystonevalve.com/data/content/cache/cache.php?mode=read']

Name

www.sinae.or.kr

Pattern Type

stix

Pattern

[hostname:value = 'www.sinae.or.kr']

Name

swt-keystonevalve.com

Pattern Type

stix

Pattern

[domain-name:value = 'swt-keystonevalve.com']

Name

www.gongsilbox.com

Pattern Type

stix

Pattern

[hostname:value = 'www.gongsilbox.com']

Name

www.daehang.com

Pattern Type

stix

Pattern

[hostname:value = 'www.daehang.com']

Name

ksmarathon.com

Pattern Type

stix

Pattern

[domain-name:value = 'ksmarathon.com']

Name

http://ksmarathon.com/admin/excel2.asp

Description

HTML document, ISO-8859 text, with CRLF line terminators
fd9e4b112b950d8c8221bf344e37a9c4a7a9159f42a19e75b0b440649e99ef79

Pattern Type

stix

Pattern

[url:value = 'http://ksmarathon.com/admin/excel2.asp']

Name

detailsecno.do

Pattern Type

stix

Pattern

[domain-name:value = 'detailsecno.do']

Name

www.coupontreezero.com

Pattern Type

stix

Pattern

[hostname:value = 'www.coupontreezero.com']

Intrusion-Set

Name
Lazarus

Malware

Name
Lazarus

Domain-Name

Value
detailsecno.do
ksmarathon.com
swt-keystonevalve.com

Hostname

Value
www.coupontreezero.com
www.sinae.or.kr
www.daehang.com
www.bcdm.or.kr
www.hmedical.co.kr
www.gongsilbox.com
www.materic.or.kr

Url

Value
https://www.bcdm.or.kr/board/type3_D/edit.asp
https://www.hmedical.co.kr/include/edit.php
https://www.coupontreezero.com/include/bottom.asp
https://www.daehang.com/member/logout.asp
https://www.materic.or.kr/files/board/equip/equip_ok.asp
https://www.gongsilbox.com/board/bbs.asp
https://swt-keystonevalve.com/data/content/cache/cache.php?mode=read
http://ksmarathon.com/admin/excel2.asp
http://www.sinae.or.kr/sub01/index.asp

External References

- https://otx.alienvault.com/pulse/6490761db8416aad20dd9404
- https://asec.ahnlab.com/en/54195/