BLOG

sfrutta una vulnerabilità zero-day

This blog looks at how the cyber-criminal group APT41 exploited a zero-day vulnerability, and examines how Darktrace's AI detected and investigated the threat at machine speed.

Executive summary

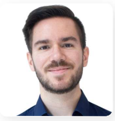
- Darktrace detected several highly targeted attacks in early March, well before any associated signatures had become available. Two weeks later, the attacks were attributed to Chinese threat-actor APT41.
- APT41 exploited the Zoho ManageEngine zero-day vulnerability CVE-2020-10189. Darktrace automatically detected and reported on the attack in its earliest stages, enabling customers to contain the threat before it could make an impact.
- The intrusions described here were part of a wider campaign aiming to gain initial access to as many companies as possible during the window of opportunity presented by CVE-2020-10189.
- The reports generated by Darktrace highlighted and delineated every aspect of the incident in the form of a meaningful security narrative. Even a junior responder could have reviewed this output and acted on this zero-day APT attack in under 5 minutes.

Fighting APT41's global attack

In early March, Darktrace detected several advanced attacks targeting customers in the US and Europe. A majority of these customers are in the legal sector. The attacks shared the same Techniques, Tools & Procedures (TTPs), targeting public-facing servers and exploiting recent high-impact vulnerabilities. Last week, FireEye attributed this suspicious activity to the Chinese cyber espionage group APT41.

This campaign used the Zoho ManageEngine zero-day vulnerability CVE-2020-10189 to get access to various companies, but little to no follow-up was detected after initial intrusion. This activity indicates a broad-brush campaign to get initial access to as many target companies as possible during the zero-day window of opportunity.

ABOUT THE AUTHOR



Max Heinemeyer
Chief Product Officer

Max is a cyber security expert with over a decade of experience in the field, specializing in a wide range of areas such as Penetration Testing, Red-Teaming, SIEM and SOC consulting and hunting Advanced Persistent Threat (APT) groups. At Darktrace, Max is closely involved with Darktrace's strategic customers & prospects. He works closely with the R&D team at Darktrace's Cambridge UK headquarters, leading research into new AI innovations and their various defensive and offensive applications. Max's insights are regularly featured in international media outlets such as the BBC, Forbes and WIRED. When living in Germany, he was an active member of the Chaos Computer Club. Max holds an MSc from the University of Duisburg-Essen and a BSc from the Cooperative State University Stuttgart in International Business Information Systems.

SHARE THIS ARTICLE

in 𝕏 f

The malicious activity observed by Darktrace took place late on Sunday March 8, 2020 and in the morning of March 9, 2020 (UTC), broadly in line with office hours previously attributed to the Chinese cyber espionage group APT41.

The graphic below shows an exemplary timeline from one of the customers targeted by APT41. The attacks observed in other customer environments are identical.

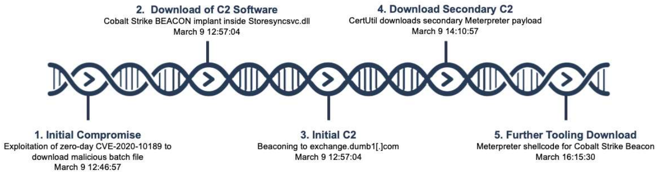

2. Download of C2 Software
Cobalt Strike BEACON implant inside Storesyncsvc.dll
March 9 12:57:04
4. Download Secondary C2
CertUtil downloads secondary Meterpreter payload
March 9 14:10:57
1. Initial Compromise
Exploitation of zero-day CVE-2020-10189 to download malicious batch file
March 9 12:46:57
3. Initial C2
Beaconing to exchange.dumb1[.]com
March 9 12:57:04
5. Further Tooling Download
Meterpreter shellcode for Cobalt Strike Beacon
March 16:15:30

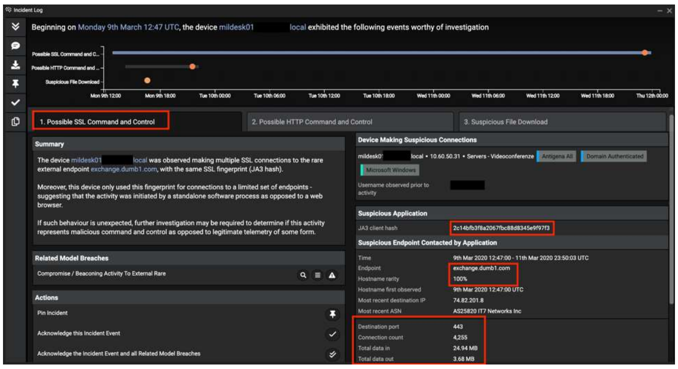
Figure 1: A timeline of the attack

Technical analysis

The attack described here centered around the Zoho ManageEngine zero-day vulnerability CVE-2020-10189. Most of the attack appears to have been automated.

We observed the initial intrusion, several follow-up payload downloads, and command and control (C2) traffic. In all cases, the activity was contained before any later steps in the attack lifecycle, such as lateral movement or data exfiltration, were identified.

The below screenshot shows an overview of the key AI Analyst detections reported. Not only did it report on the SSL and HTTP C2 traffic, but it also reported on the payload downloads:



Beginning on Monday 9th March 12:47 UTC, the device mildesk01 [redacted] local exhibited the following events worthy of investigation

1. Possible SSL Command and Control | 2. Possible HTTP Command and Control | 3. Suspicious File Download

Summary

The device mildesk01 [redacted] local was observed making multiple SSL connections to the rare external endpoint exchange.dumb1.com, with the same SSL fingerprint (JA3 hash).

Moreover, this device only used this fingerprint for connections to a limited set of endpoints - suggesting that the activity was initiated by a standalone software process as opposed to a web browser.

If such behaviour is unexpected, further investigation may be required to determine if this activity represents malicious command and control as opposed to legitimate telemetry of some form.

Related Model Breaches

Compromise / Beaconing Activity To External Rare

Actions

Pin Incident

Acknowledge this Incident Event

Acknowledge the Incident Event and all Related Model Breaches

Device Making Suspicious Connections

mildesk01 [redacted] local • 10.60.50.31 • Servers - Videoconferenze Antigena All Domain Authenticated Microsoft Windows

Username observed prior to activity [redacted]

Suspicious Application

JA3 client hash 2c14bfb3f8a2067fbc88d8345e9f97f3

Suspicious Endpoint Contacted by Application

Time	9th Mar 2020 12:47:00 - 11th Mar 2020 23:50:03 UTC
Endpoint	exchange.dumb1.com
Hostname rarity	100%
Hostname first observed	9th Mar 2020 12:47:00 UTC
Most recent destination IP	74.82.201.8
Most recent ASN	AS25820 IT7 Networks Inc
Destination port	443
Connection count	4,255
Total data in	24.94 MB
Total data out	3.68 MB

Figure 2: SSL C2 detection by Cyber AI Analyst

Stay up to date on the latest industry news and insights.

Indirizzo e-mail

First Name

Last Name

Organization name

You can unsubscribe at any time. Privacy Policy

□ 进行人机身份验证 reCAPTCHA 隐私权 - 使用条款

Subscribe

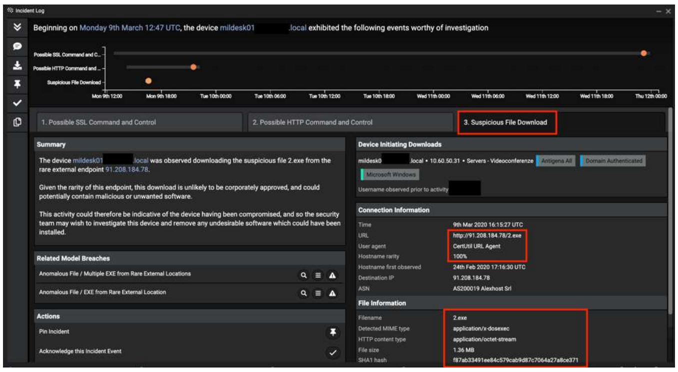
TRENDING BLOGS

1 Securing the Cloud Starts By Understanding It
Nov 1, 2023

2 Using AI to Help Humans Function Better During a Cyber Crisis
Sep 19, 2023

3 When Hallucinations Become Reality: An Exploration of AI Package Hallucination Attacks
Oct 30, 2023

4 Darktrace/Email in Action: Why AI-Driven Email Security is the Best Defense Against Sustained Phishing Campaigns
Sep 26, 2023



Beginning on Monday 9th March 12:47 UTC, the device mildesk01[redacted].local exhibited the following events worthy of investigation

Summary

The device mildesk01[redacted].local was observed downloading the suspicious file 2.exe from the rare external endpoint 91.208.184.78.

Given the rarity of this endpoint, this download is unlikely to be corporately approved, and could potentially contain malicious or unwanted software.

This activity could therefore be indicative of the device having been compromised, and so the security team may wish to investigate this device and remove any undesirable software which could have been installed.

Related Model Breaches

Anomalous File / Multiple EXE from Rare External Locations

Anomalous File / EXE from Rare External Location

Actions

Pin Incident

Acknowledge this Incident Event

Device Initiating Downloads

mildesk0[redacted].local • 10.60.50.31 • Servers - Videoconferenze Antigena All Domain Authenticated Microsoft Windows

Username observed prior to activity [redacted]

Connection Information

Time	9th Mar 2020 16:15:27 UTC
URL	http://91.208.184.78/2.exe
User agent	CertUtil URL Agent
Hostname rarity	100%
Hostname first observed	24th Feb 2020 17:16:30 UTC
Destination IP	91.208.184.78
ASN	AS200019 Alexhost Srl

File Information

Filename	2.exe
Detected MIME type	application/x-dosexec
HTTP content type	application/octet-stream
File size	1.36 MB
SHA1 hash	f87ab33491ee84c579cab9d87c7064a27a8ce371

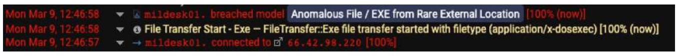
Figure 3: Payload detection by Cyber AI Analyst

Initial compromise

The initial compromise began with the successful exploitation of the Zoho ManageEngine zero-day vulnerability CVE-2020-10189. Following the initial intrusion, the Microsoft BITSAdmin command line tool was used to fetch and install a malicious Batch file, described below:

install.bat (MD5: 7966c2c546b71e800397a67f942858d0) from infrastructure 66.42.98[.]220 on port 12345.

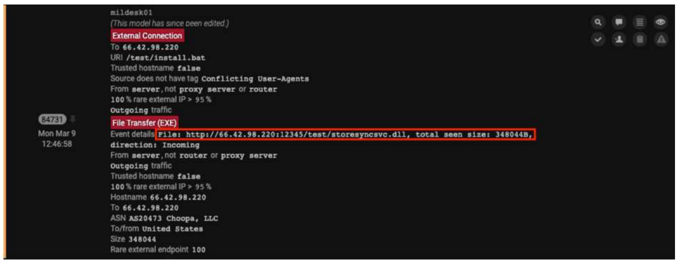
Source: 10.60.50.XX
Destination: 66.42.98[.]220
Destination Port: 12345
Content Type: application/x-msdownload
Protocol: HTTP
Host: 66.42.98[.]220
URI: /test/install.bat
Method: GET
Status Code: 200



```
Mon Mar 9, 12:46:58  ▾ mildesk01. breached model Anomalous File / EXE from Rare External Location [100% (now)]
Mon Mar 9, 12:46:58  ▾ File Transfer Start - Exe — FileTransfer::Exe file transfer started with filetype (application/x-dosexec) [100% (now)]
Mon Mar 9, 12:46:57  ▾ → mildesk01. connected to 66.42.98.220 [100%]
```

Figure 4: Outbound connection fetching batch file

Shortly after the initial compromise, the first stage Cobalt Strike Beacon LOADER was downloaded.



```
84731
Mon Mar 9
12:46:58
mildesk01
(This model has since been edited.)
External Connection
To 66.42.98.220
URI /test/install.bat
Trusted hostname false
Source does not have tag Conflicting User-Agents
From server, not proxy server or router
100 % rare external IP > 95 %
Outgoing traffic
File Transfer (EXE)
Event details File: http://66.42.98.220:12345/test/storesyncsvc.dll, total seen size: 348044B,
direction: Incoming
From server, not router or proxy server
Outgoing traffic
Trusted hostname false
100 % rare external IP > 95 %
Hostname 66.42.98.220
To 66.42.98.220
ASN AS20473 Choopa, LLC
To/from United States
Size 348044
Rare external endpoint 100
```

Figure 5: Detection of the Cobalt Strike Beacon LOADER

Command and Control traffic

Interestingly, TeamViewer activity and the download of Notepad++ was taking place at the same time as the C2 traffic was starting in some of the customer attacks. This

5

Akira Ransomware: How Darktrace Foiled Another Novel Ransomware Attack

Sep 13, 2023

indicates APT41 trying to use familiar tools instead of completely 'Living off the Land'.

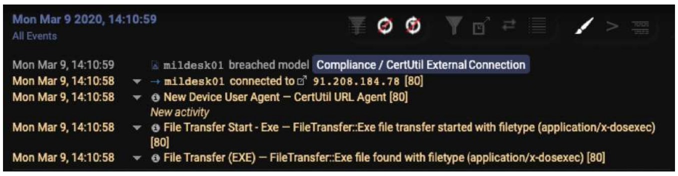
Storesyncsvc.dll was a Cobalt Strike Beacon implant (trial-version) which connected to exchange.dumb1[.]com. A successful DNS resolution to 74.82.201[.]8 was identified, which Darktrace discerned as a successful SSL connection to a hostname with Dynamic DNS properties.

Multiple connections to exchange.dumb1[.]com were identified as beaconing to a C2 center. This C2 traffic to the initial Cobalt Strike Beacon was leveraged to download a second stage payload.

Interestingly, TeamViewer activity and the download of Notepad++ was taking place at the same time as the C2 traffic was starting in some of the customer attacks. This indicates APT41 trying to use familiar tools instead of completely 'Living off the Land'. There is at least high certainty that the use of these two tools can be attributed to this intrusion instead of regular business activity. Notepad++ was not normally used in the target customers' environments, nor was TeamViewer – in fact, the use of both applications was 100% unusual for the targeted organizations.

Attack tools download

CertUtil.exe, a command line program installed as part of Certificate Services, was then leveraged to connect externally and download the second stage payload.

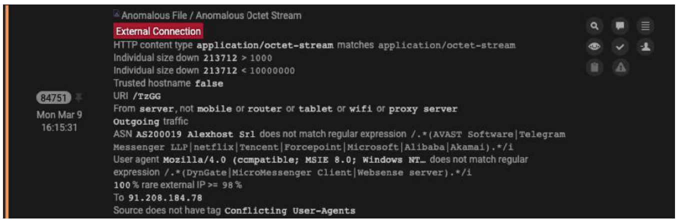


```
Mon Mar 9 2020, 14:10:59
All Events

Mon Mar 9, 14:10:59      mildesk01 breached model Compliance / CertUtil External Connection
Mon Mar 9, 14:10:58   ▾ → mildesk01 connected to 91.208.184.78 [80]
Mon Mar 9, 14:10:58   ▾ ℹ New Device User Agent — CertUtil URL Agent [80]
                        New activity
Mon Mar 9, 14:10:58   ▾ ℹ File Transfer Start - Exe — FileTransfer::Exe file transfer started with filetype (application/x-dosexec)
                        [80]
Mon Mar 9, 14:10:58   ▾ ℹ File Transfer (EXE) — FileTransfer::Exe file found with filetype (application/x-dosexec) [80]
```

Figure 6: Darktrace detecting the usage of CertUtil

A few hours after this executable download, the infected device made an outbound HTTP connection requesting the URI /TzGG, which was identified as Meterpreter downloading further shellcode for the Cobalt Strike Beacon.



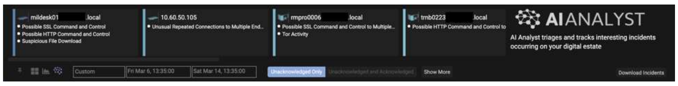
```
              Anomalous File / Anomalous Octet Stream
              External Connection
              HTTP content type application/octet-stream matches application/octet-stream
              Individual size down 213712 > 1000
              Individual size down 213712 < 10000000
              Trusted hostname false
 84751        URI /TzGG
Mon Mar 9     From server, not mobile or router or tablet or wifi or proxy server
 16:15:31     Outgoing traffic
              ASN AS200019 Alexhost Srl does not match regular expression /.*(AVAST Software|Telegram
              Messenger LLP|netflix|Tencent|Forcepoint|Microsoft|Alibaba|Akamai).*/i
              User agent Mozilla/4.0 (ccmpatible; MSIE 8.0; Windows NT… does not match regular
              expression /.*(DynGate|MicroMessenger Client|Websense server).*/i
              100 % rare external IP >= 98 %
              To 91.208.184.78
              Source does not have tag Conflicting User-Agents
```

Figure 7: Detection associated with Meterpreter activity. No lateral movement or significant data exfiltration was observed.

How Cyber AI Analyst reported on the zero-day exploit

Darktrace not only detected this zero-day attack campaign, but Cyber AI Analyst also saved security teams valuable time by investigating disparate security events and generating a report that immediately put them in a position to take action.

The below screenshot shows the AI Analyst incidents reported in one infected environment, over the eight days covering the intrusion period. The first incident on the left represents the APT activity described here. The other five incidents are independent of the APT activity and not as severe.



mildesk01[redacted].local
- Possible SSL Command and Control
- Possible HTTP Command and Control
- Suspicious File Download

10.60.50.105
- Unusual Repeated Connections to Multiple End...

rmpro0006[redacted].local
- Possible SSL Command and Control to Multiple...
- Tor Activity

tmb0223[redacted].local
- Possible HTTP Command and Control to

AI ANALYST

AI Analyst triages and tracks interesting incidents occurring on your digital estate

Custom | Fri Mar 6, 13:35:00 | Sat Mar 14, 13:35:00

Figure 8: The security incidents surfaced by AI Analyst

AI Analyst reported on six incidents in total over the eight-day period. Each AI Analyst incident includes a detailed timeline and summary of the incident, in a concise format that takes an average of two minutes to review. This means that with Cyber AI Analyst, even a non-technical person could have actioned a response to this sophisticated, zero-day incident in less than five minutes.

Conclusion

Without public Indicators of Compromise (IoCs) or any open-source intelligence available, targeted attacks are incredibly difficult to detect. Moreover, even the best detections are useless if they cannot be actioned by a security analyst at an early stage. Too often this occurs because of an overwhelming volume of alerts, or simply because the skills barrier to triage and investigation is too high.

This appears to be a broad campaign to gain initial access to many different companies and sectors. While very sophisticated in nature, the threat sacrificed stealth for speed by targeting many companies at the same time. APT41 wanted to utilize the limited window of opportunity that the Zoho zero-day provided before IT staff starts patching.

Darktrace's Cyber AI is specifically designed to detect the subtle signs of targeted, unknown attacks at an early stage, without relying on prior knowledge or IoCs. It achieves this by continuously learning the normal patterns of behavior for every user, device, and associated peer group from scratch, and 'on the job'.

In the face of this zero-day attack campaign, the AI's ability to (a) detect unknown threats with self-learning AI and (b) augment strained responders with AI-driven investigations and reporting proved crucial. Indeed, it ensured that the attacks were swiftly contained before escalating to the later stages of the attack lifecycle.

Indicators of Compromise

Selection of Darktrace model breaches:

- Anomalous File / Script from Rare External
- Anomalous File / EXE from Rare External Location
- Compromise / SSL to DynDNS
- Compliance / CertUtil External Connection
- Anomalous Connection / CertUtil Requesting Non Certificate
- Anomalous Connection / CertUtil to Rare Destination
- Anomalous Connection / New User-Agent to IP Without Hostname
- Device / Initial Breach Chain Compromise
- Compromise / Slow Beaconing Activity To External Rare
- Compromise / Beaconing Activity To External Rare
- Anomalous File / Numeric Exe Download
- Device / Large Number of Model Breaches
- Anomalous Server Activity / Rare External from Server
- Compromise / Sustained TCP Beaconing Activity To Rare Endpoint
- Compliance / Remote Management Tool On Server

The below screenshot shows Darktrace model breaches occurring together during the compromise of one customer:

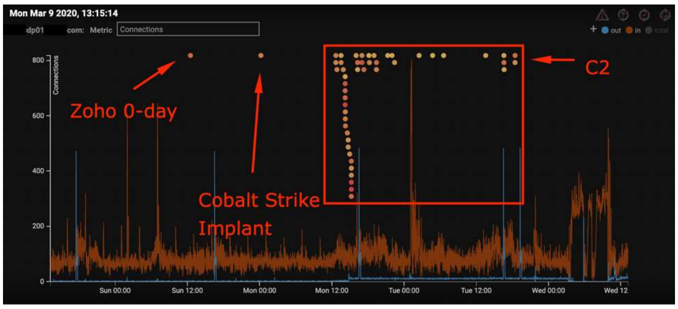


Figure 9: Darktrace model breaches occurring together

BLOG

OT

Three ways AI secures OT & ICS from Cyber Attacks

09 Jan 2024

What is OT and ICS?

Operational technologies and industrial control systems are the networked technologies used for the automation of physical processes. These are the technologies that allow operators to control processes and retrieve real time process data from a factory, rail system, pipeline, and other industrial processes.

The role of AI in defending OT/ICS networks

While largely adopted by industrial organizations, OT is utilized by Critical Infrastructures, these being the industries that directly affec...

Continue reading ⟶

ABOUT THE AUTHOR

Oakley Cox
Analyst Technical Director, APAC

BLOG

Inside the SOC

Countering the Cartel: Darktrace's Investigation into CyberCartel Attacks Targeting Latin America

08 Jan 2024

ABOUT THE AUTHOR

Alexandra Sentenac

Cyber Analyst

Introduction

In September 2023, Darktrace published its first Half-Year Threat Report, highlighting Threat Research, Security Operation Center (SOC), model breach, and Cyber AI Analyst analysis and trends across the Darktrace customer fleet. According to Darktrace's Threat Report, the most observed threat type to affect Darktrace customers during the first half of 2023 was Malware-as-a-Service (Maas). The report highlighted a growing trend where malware strains, specifically in the MaaS ecosystem, "use cross-functional components from other strains as part of their evolution and...

Continue reading ⟶

DARKTRACE

Evolving threats call for evolved thinking™

Italiano

Prodotti

Darktrace PREVENT

Darktrace DETECT

Darktrace RESPOND

Darktrace HEAL

Copertura di base

Nuvola

Applicazioni

Email

Endpoint

Zero Trust

Rete

OT

Centro di ricerca sull'intelligenza artificiale

Panoramica

Azienda

Panoramica dell'azienda

News

Investitori

Carriera

Partner

Panoramica dei partner

Partner tecnologici

Integrazioni

Risorse

All Resources

Blog

Eventi

Webinar

Glossary

Legale

Informativa sulla privacy

Informativa sui cookie

Dichiarazione sulla legge sulla schiavitù moderna

Strategia fiscale pubblica

Politica di divulgazione delle vulnerabilità

Mappa del sito