

# Catching APT41 exploiting a zero-day vulnerability

 [darktrace.com/en/blog/catching-apt-41-exploiting-a-zero-day-vulnerability/](https://darktrace.com/en/blog/catching-apt-41-exploiting-a-zero-day-vulnerability/)



Max Heinemeyer, Director of Threat Hunting



## 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 by APT41 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.

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.



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:



Figure 2: SSL C2 detection by Cyber AI Analyst



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



Figure 4: Outbound connection fetching batch file

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



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 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.



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.



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.



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

---

While very sophisticated in nature, APT41 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.

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 by APT41 to gain initial access to many different companies and sectors. While very sophisticated in nature, APT41 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 APT41's recent 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 Beaconsing Activity To External Rare
- Compromise / Beaconsing 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 Beaconsing 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

Network IoCs:

IoC	Comment
-----	---------

---

66.42.98[.]220	Initial compromise and payload downloads
74.82.201[.]8	DNS resolution for C2 domain
exchange.dumb1[.]com	Main C2 domain
91.208.184[.]78	Secondary Cobalt Strike C2

Host IoCs:

IoC	Comment
Filename	MD5 Hash
install.bat	7966c2c546b71e800397a67f942858d0
storesyncsvc.dll	5909983db4d9023e4098e56361c96a6f
2.exe	3e856162c36b532925c8226b4ed3481c
TzGG	659bd19b562059f3f0cc978e15624fd9

## MITRE ATT&CK techniques observed

Initial Access	T1190 – Exploit Public-Facing Application T1133 – External Remote Services
Execution	T1064 — Scripting
Persistence	T1050 – New Service T1197 – BITS Jobs
Privilege Escalation	T1068 — Exploitation for Privilege Escalation
Defense Evasion	T1055 – Process Injection T1197 – BITS Jobs
Discovery	
Exfiltration	
Command and Control	T1043 – Commonly Used Ports T1071 – Standard Application Layer Protocol T1132 – Data Encoding T1008 – Fallback Channels

**Max Heinemeyer**

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 oversees global threat hunting efforts, working with strategic customers to investigate and respond to cyber-threats. 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.