Deep Dive into a Corporate Espionage Operation

businessinsights.bitdefender.com/deep-dive-into-a-corporate-espionage-operation

Martin Zugec

By **Martin Zugec** / Aug 31, 2022

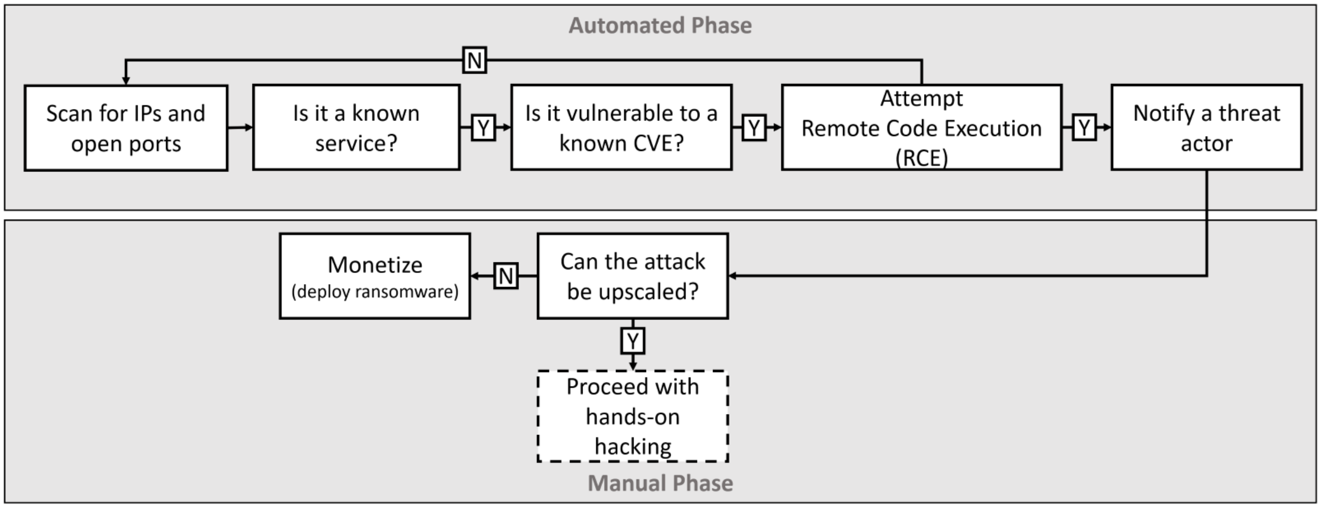
Corporate espionage, also known as industrial espionage, is espionage conducted for commercial or financial purposes. One of the common misconceptions is that espionage is affecting only large corporations or government entities, but it is more common than expected. In this article, we provide an analysis of one such exfiltration and explain why these attacks are on the rise.

In the last few years, we have seen a dramatic shift in the level of sophistication of cyber attacks, mostly thanks to the introduction of the profit-sharing business model for financially motivated threat actors. However, not all stages of the kill chain have received the same attention from threat actors – the focus has been mostly on developing the attack after the initial compromise, focusing on reconnaissance, lateral movement, and extortion methods. The three attack vectors are still dominating the initial compromise:

- Leaked or default/weak credentials (62% of actionable alerts by our Managed Detection and Response service)
- Phishing attacks
- Vulnerability exploits

But one of these things is not like the others. Vulnerability exploits are not relying on the human element, instead, they are using automated scanners to identify and compromise internet-facing systems with unpatched vulnerabilities. According to the latest Data Breach Investigations Report 2022 (DBIR 2022), the number of **security breaches caused by**

vulnerability exploits has doubled in the last year. This trend can be explained by the increased popularity of hybrid attacks – a type of attack where the initial compromise is opportunistic and relies on automated scanners but is then triaged by a human operator to determine if it’s worth further development.


Automated Phase
N
Scan for IPs and open ports
Is it a known service?
Y
Is it vulnerable to a known CVE?
Y
Attempt Remote Code Execution (RCE)
Y
Notify a threat actor
Monetize (deploy ransomware)
N
Can the attack be upscaled?
Y
Proceed with hands-on hacking
Manual Phase

Hybrid attacks are on the rise, combining the automated initial compromise with hands-on triage.

Data exfiltration and the threat of industrial espionage

This “upscaling” of attacks can take different forms – for example, even a small company with few computers can have highly valuable data, for instance, lawyers working with celebrities or politicians. Or a company can be part of the supply chain for a much larger corporation, becoming a prime target for Ransomware-as-a-Service groups. Understanding how modern threat actors operate, it should not be surprising that business partners were involved in 39% of the data breaches last year (source: DBIR 2022). We expect this trend to continue, as threat actors are focusing more on a breach of confidentiality (data exfiltration) than a breach of availability (deploying ransomware). While we are still using the label "Ransomware-as-a-Service" for these profit-sharing criminal organizations, many of them are not even deploying ransomware anymore (for example Karakurt). With the rise of hybrid attacks, even small companies are targeted by sophisticated threat actors, such as RaaS affiliates specialized in enterprise targets, or state-sponsored APT groups.

In this deep dive, we analyze the recent industrial espionage operation targeting a small (under 200 employees) technology company based in the United States. The attack was focused on information exfiltration and spans several months. A vast network of several hundred IP addresses (most of them originated from China) was used as part of this attack. Small and medium-sized companies often lack detection and response capabilities, the most effective defense mechanism when dealing with sophisticated threat actors. We share this research to help other companies to identify their blind spots and become more cyber resilient.

Anatomy of an attack

Our security researchers from Bitdefender Labs have released a research paper Hiding in the Shadows: Investigation of a Corporate Espionage Attack with full details. The anatomy of an attack that follows is the summary of this research.

Initial compromise

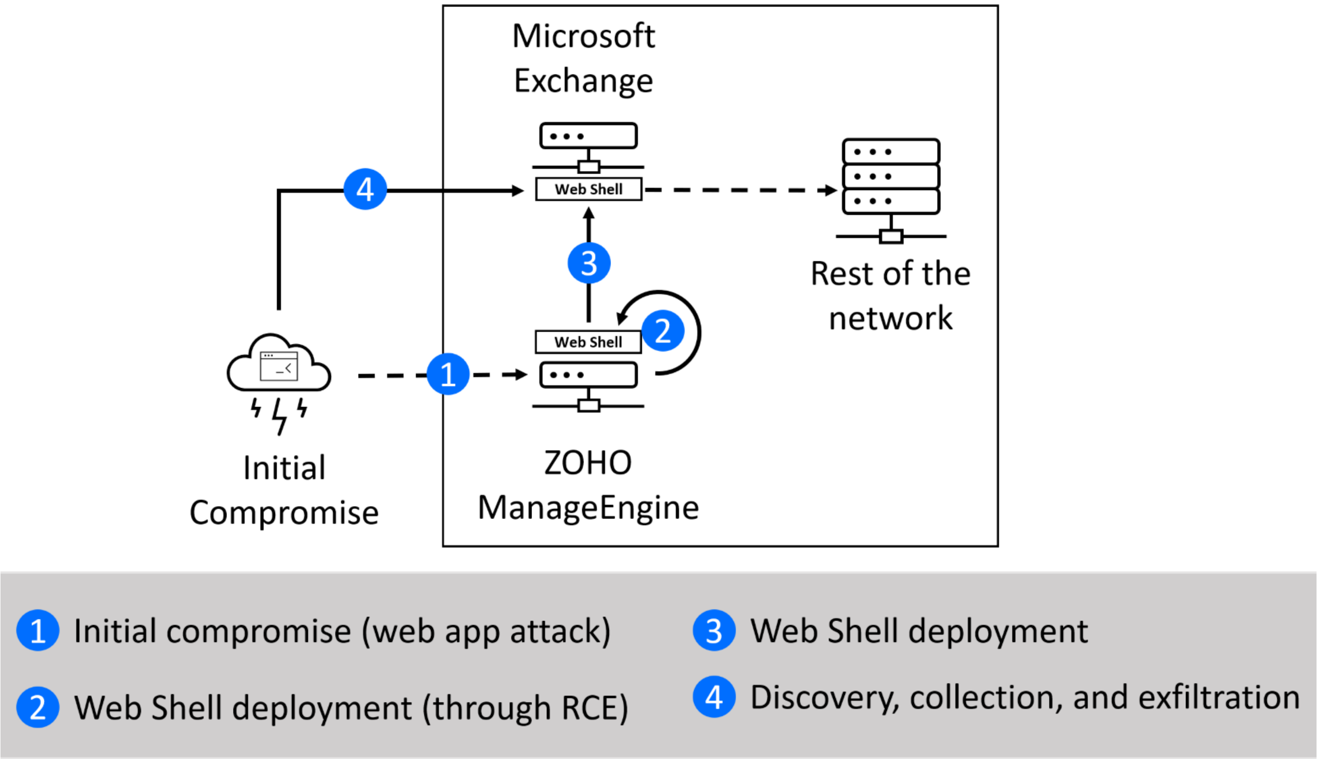
The initial infection vector was an internet-facing instance of ZOHO ManageEngine ADSelfService Plus web server exploited via a known unpatched vulnerability CVE-2021-40539. This is one of the top 15 routinely exploited vulnerabilities (source: CISA), allowing a threat actor to bypass a security authentication and execute arbitrary code.

Surprisingly, attacking basic web applications using one of the well-known vulnerabilities is an effective method for nation-state actors to compromise networks. This is a low-cost/high-value attack vector, and over 30% of web application attacks are related to espionage (a significantly higher number than any other attack vector). When prioritizing your security strategy, make sure these routinely exploited vulnerabilities are handled as a top priority. You can read more details about this vulnerability in the research How to exploit CVE-2021-40539 on ManageEngine ADSelfService Plus.

After gaining access to this system, threat actors deployed a web shell in a directory accessible from the internet. A web shell is a malicious shell-like interface (usually written in web development languages such as JSP, PHP…) that is used to access a web server remotely, providing a threat actor with access even after the exploited vulnerability is fixed. For this operation, a combination of different web shells was used – Tunna, ReGeorg, and China Chopper Webshell.

Establishing persistence

After the initial foothold was established, threat actors continued with system discovery, identifying and locating other machines and file shares on the network. Microsoft Exchange server was compromised, and another set of web shells was deployed on this server. Threat actors abandoned the initial compromised server in favor of this Exchange server, which became their base of operations.



Preparing staging environment for the exfiltration

Once a backup access vector was set in place, an extensive discovery phase was started. Threat actors used a range of tools to obtain access to credentials, including a signed version of DCSync module of Mimikatz, Windows Vault Password Decryptor, Sqldumper.exe utility, NTDSDumpEx, and export of SAM registry hives. To capture more credentials, threat actors enabled the Digest Authentication protocol (WDigest) in the registry. This was a legacy protocol used in Windows Server 2003 and older operating systems that requires storing clear-text passwords in the memory. By enabling this protocol, threat actors can harvest not only password hashes, but also clear text passwords for all users authenticated against a server with this protocol enabled.

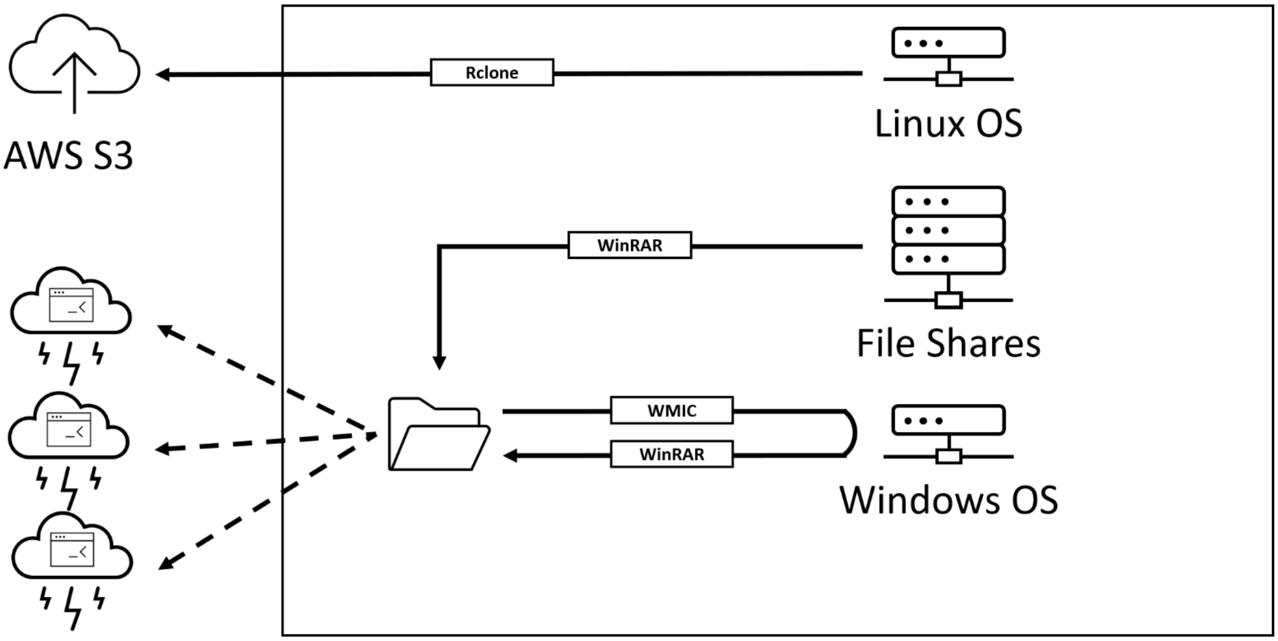
```
cmd /c cd /d “C:\inetpub\wwwroot\aspnet_client\css\”&reg add
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /d 1 /f&echo [S]&cd&echo [E]
```

Data exfiltration

Sensitive information was collected, including SSH keys, VPN certificates, and more. The threat actor managed to obtain plaintext credentials of a user with read access to multiple Git repositories, and the source code was downloaded using a tool called `git2.exe`. To exfiltrate all this collected data, threat actors used `rar.exe` utility to split files into a collection of 2GB archives. Both data and headers were encrypted for these archive files and protected by the password `CIA@NSA@FBI` (very subtle). Before exfiltration, all files were renamed from `.rar` to `.jpg` and stored in a folder accessible from the internet.

To collect all this data, a few different methods were used, depending on the type of target machine. For file shares, WinRAR was used to compress files and pull archives to the central exfiltration folder (pulling data). For Windows OS machines, WMI was used to start the remote WinRAR process (pushing data from the target machine). Finally, for Linux OS machines, a different approach was used – Rclone tool uploaded files directly to the Amazon S3 bucket.

After all the files were saved in the central exfiltration folder, exfiltration was launched using normal HTTP GET requests (the folder was accessible from the internet). These HTTP requests were performed in a highly parallel manner – threat actors used HTTP Range Header, so multiple IPs can concurrently download different segments of a single file. Over 650 IPs were used to exfiltrate this data, most of them can be traced back to China.



Different data exfiltration flows

Conclusion & recommendations

The best protection against modern cyber-attacks is a defense-in-depth architecture. Start with reducing your attack surface, focusing on patch management (not only for Windows but for all applications and internet-exposed services), and detection of misconfigurations. Read our technical brief to learn about GravityZone Patch Management solution.

The next security layer should be reliable world-class prevention controls that can eliminate most security incidents, using multiple layers of security, including IP/URL reputation for all endpoints, and protection against fileless attacks.

Implementing IP, domain, and URL reputation, powered by Bitdefender's threat intelligence solution, is one of the most effective methods to stop automated vulnerability exploits. According to analysis in the Data Breach Investigations Report 2022, only 0.4% of the IPs that attempted RCEs were not seen in one of the previous attacks. Block bad IPs, domains, or URLs on all devices, including endpoints, and prevent a security breach in your business environment.

Finally, for the few incidents that get through your defenses, lean on security operations, either in-house or through a managed service, and leverage strong detection and response tools. Modern threat actors often spend weeks or months doing active reconnaissance on networks, generating alerts, and relying on the absence of detection and response capabilities.

Learn more about Bitdefender's XDR and MDR service offerings.

Indicators of compromise

An up-to-date and complete list of indicators of compromise is available to Bitdefender Threat Intelligence users. The currently known indicators of compromise can be found in the table below.

IPs used to access the web shells

IP Address
113[.]25[.]2[.]136
139[.]162[.]2[.]70
193[.]34[.]167[.]229
45[.]14[.]71[.]12
172[.]86[.]75[.]152
103[.]224[.]116[.]98
113[.]25[.]10[.]69

58[.]221[.]37[.]66
125[.]79[.]201[.]69
140[.]249[.]254[.]251
222[.]67[.]12[.]181
112[.]49[.]92[.]234
182[.]138[.]144[.]147
111[.]126[.]218[.]45
171[.]8[.]217[.]156
117[.]162[.]164[.]55
113[.]2[.]174[.]149
49[.]81[.]61[.]251
39[.]128[.]220[.]139
39[.]144[.]17[.]62
39[.]144[.]4[.]66
221[.]178[.]126[.]191
59[.]163[.]248[.]170
39[.]144[.]5[.]87
59[.]163[.]248[.]162

39[.]144[.]14[.]38
221[.]178[.]124[.]233
67[.]227[.]206[.]162
221[.]178[.]127[.]152
39[.]144[.]4[.]160

URLs

URL
https://app.jetboatpilot[.]com/utils/optimize/ver.ico
http://node-sdk-sample-760723cc-b7e7-43ef-9f5b-9eca39acdefe.s3.us-west-1.amazonaws[.]com/git2.exe

Files

File Path/Name	SHA256
C:\inetpub\wwwroot\aspnet_client\css\rr.aspx	742a27fb2a87e2c660fea0bb8184b53e
C:\inetpub\wwwroot\aspnet_client\css\ex.aspx	84b5e2ac1846d268f1cf9581b63bf953
test.jsp	182d244ab4cd63e63997c0ec5d34f320
y.jsp	28e0f31c506b346b8462f61b4903dcb3
C:\ManageEngine\ADSelfService Plus\webapps\adssp\images\ mobile\mapp\m.exe	6572fc009a714fefc92dafcb2250f83d

C:\ManageEngine\ADSelfService Plus\bin\vm.exe	c8460622d893c5753b44a3ac08f55b4f
C:\Windows\Temp\nt.exe	ab6414b83b23807dd530d250829c8bc1
ver.ico	fe54e8952f4a24d0747078ee8983ff4d
test.jsp	57988b776d80b73ecc7640c72fc4f4a6
nav_working.jsp	f23436e941af00ae05ad709a7e1da8e1
tot.jsp	c9951e1646f68e418a186480c31eb00e
ad.txt	c951158b74ec5b1869d0ff9ae7ae63f9
t.jsp	eb4f89071009c72248ae26d46900d0f2
ttt.jsp	2b65120a2d5703d2a042039a997b1284
tot.jsp	2b65120a2d5703d2a042039a997b1284

CONTACT AN EXPERT