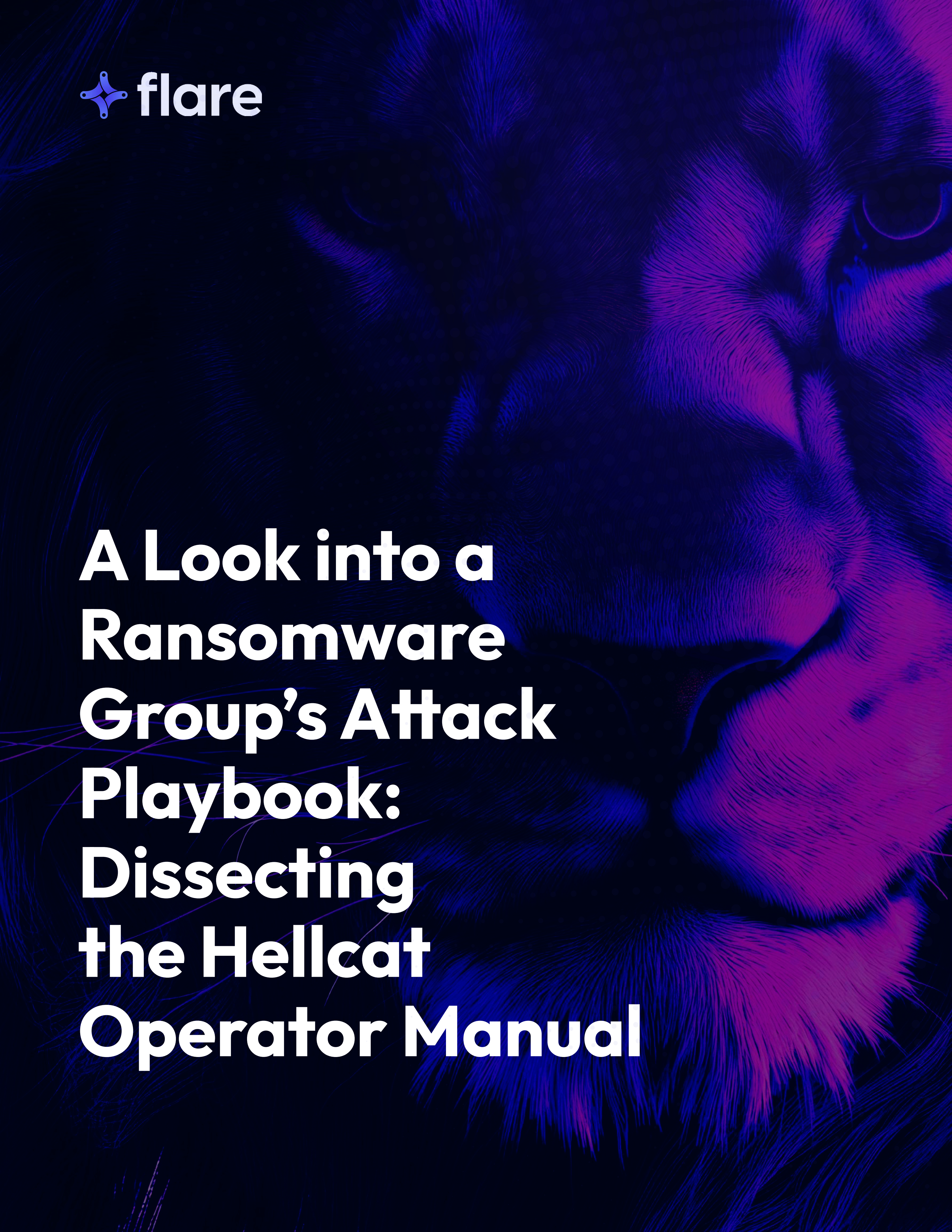


flare

A Look into a Ransomware Group's Attack Playbook: Dissecting the Hellcat Operator Manual

“Think like a threat actor.”

Nearly every security professional has heard this at some point, especially red teamers and penetration testers. In that context, the phrase often means looking at vulnerabilities across the attack surface that threat actors can leverage to gain unauthorized access. Logically, security teams understand that most attackers are financially motivated.

While many organizations worry about zero-day attacks leveraging previously unknown vulnerabilities, most threat actors want to gain easy access to sensitive information. Malicious actors typically look for low effort attack methods that provide the highest revenue opportunities, essentially looking for a solid return on investment.

Flare Research has analyzed what security teams can learn from the leaked Hellcat ransomware group’s operator manual (a blueprint for their attacks). While the manual was originally a closely guarded secret for other threat actors within their group to learn from, it can now offer a wealth of knowledge to security teams. It’s dated to 2024, but it can still be incredibly valuable if organizations haven’t updated security measures since before then or would like to review their current security practices.

The Hellcat ransomware group’s manual is confirmation that threat actors, even ones capable of sophisticated attack methods, will focus on the easiest path possible.

Read below for what we at Flare Research gathered from this ransomware group’s manual and what security teams can do to boost their organizations’ defenses.

What is Hellcat?

Hellcat was a sophisticated Ransomware-as-a-Service (RaaS) organization that started off in 2024 from Breach Forums, and targeted large organizations and their infrastructures. While primarily administered by a threat actor with the online handle Miyako, the organization consisted of various threat actors.

Typically, Hellcat leveraged known exploits and designed scripts so they could deploy their own malware. For a while, the group attempted to run an affiliate model, recruiting other threat actors to deploy the attacks and splitting the ransom. In an effort to streamline these malicious actor operations, Miyako created a manual explaining how they conducted attacks so others could easily follow the same tactics.

While Hellcat was an opportunistic ransomware group, it typically targeted financial services, healthcare, and Industrial Control Systems (ICS).

Why is the Hellcat Manual Valuable?

As part of their operations, many cybercriminal organizations provide manuals to their affiliates. However, the groups typically treat these like trade secrets to keep competitors from copying their methodologies. For example, in 2023, two manuals from Bastlord aka Fisheye reached the public and gave insight into the LockBit affiliate operations.

The Hellcat manual offers another opportunity to study threat actor TTPs. By studying this manual, security teams can understand the different tactics that Hellcat used, and enable them to better protect their environments. We will cover their three common tactics below (along with key takeaways for defenders):

- Targeting a known vulnerability
- Weaponizing a publicly available Proof of Concept (PoC)
- Automating activities

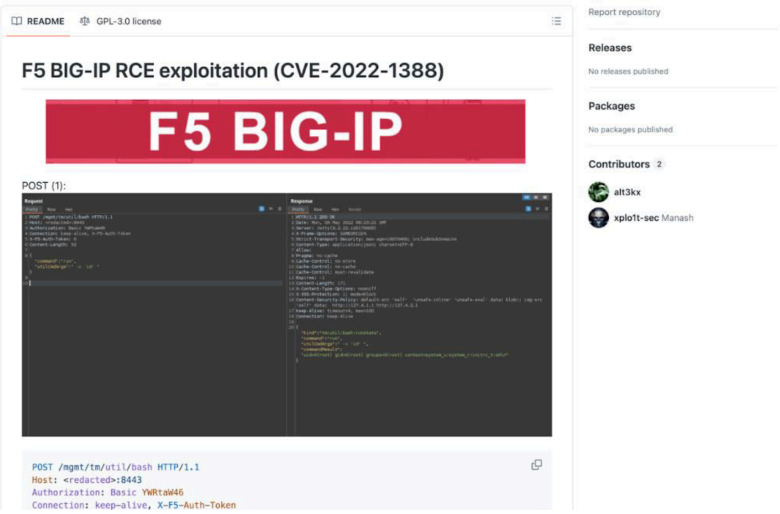
Common Tactic #1: Target a Known Vulnerability

Across three different attacks documented in Hellcat's manual, known vulnerabilities acted as the initial entrance point. Threat actors find these vulnerabilities valuable for several reasons:

- Organizations may not actively monitor the technology because the vulnerability is not currently top of mind.
- The publicly available exploits intended to help red teamers and pen testers are easy to weaponize for threat actors.

Attack Case Study: Telecommunications Company

In the alleged attack on a telecommunications company, Miyako identified a target running F5 BIG-IP. From here, the threat actors identified a vulnerability using the exploit search engine Sploitus. In this case, the vulnerability was only exploitable if misconfigured, making it a high-value target if organizations failed to apply the security update, assumed they implemented secure configurations, or failed to identify the misconfiguration.



F5 BIG-IP RCE exploitation (CVE-2022-1388)

POST (1):

```
POST /mgmt/tm/util/bash HTTP/1.1
Host: <redacted>:8443
Authorization: Basic YWRtaW46
Connection: keep-alive, X-F5-Auth-Token
```

Attack Case Study: PAN-OS

The walkthrough for the Palo Alto Networks PAN-OS attack started with a known vulnerability, CVE-2024-0012, that allowed remote code execution after bypassing authentication. In this case, Miyako targeted a popular firewall vendor to reach as many victims as possible while also compromising a critical security tool organizations use to detect attacks.

Attack Case Study: Government Server

In December 2024, Miyako identified the Financial and Asset management Agency for the Blora Regency in Indonesia running on a Webmin instance with a five-year old vulnerability, CVE-2019-15107. In this case, the vulnerability was only exploitable if misconfigured, making it a high-value target if organizations failed to apply the security update, assuming they implemented secure configurations or failed to identify the misconfiguration.

Key Takeaway for Security Teams: N-Day Vulnerabilities Are Easy Targets

An N-day vulnerability is a publicly known security weakness that either has no security update available or that organizations failed to patch appropriately. Threat actors find these vulnerabilities are valuable long after security researchers and vendors report their existence for various reasons, including:

- **Easy identification:** Threat actors scan networks for known vulnerabilities during the reconnaissance phase.
- **Breadth of targets:** Malicious actors target all organizations using a technology to expand the attack's reach.
- **Forgotten flaws:** Threat actors assume the organization failed to patch the vulnerability and subsequently forgot it could be an attack vector.

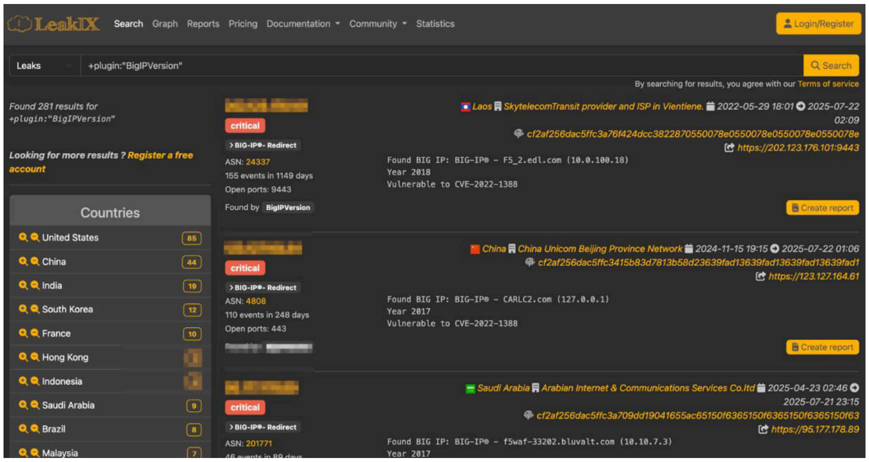
Common Tactic #2: Weaponize a Publicly Available Proof of Concept (PoC)

In the aftermath of a published vulnerability, security researchers often publicly share ways that attackers could exploit it, often sharing them in places like GitHub. The PoCs enable vulnerability and patch management teams to prioritize remediation activities. However, threat actors with the same access to these publicly available exploits can use them to complete their malicious objectives.

Attack Case Study: Telecommunications Company

Miyako took the information from Sploitus and followed it to the GitHub repository containing a PoC. According to the manual, “not all PoCs are full exploits, but this one was.”

After downloading it, they looked for a vulnerable host containing valuable information. They used LeakIX to help them find open buckets and accessible infrastructure.



+plugin:"BigIPVersion"

By searching for results, you agree with our Terms of service

Found 281 results for +plugin:"BigIPVersion"

Looking for more results ? Register a free account

Countries	
United States	85
China	44
India	19
South Korea	12
France	10
Hong Kong	[redacted]
Indonesia	[redacted]
Saudi Arabia	9
Brazil	8
Malaysia	7

[redacted]
critical
> BIG-IP®- Redirect
ASN: 24337
155 events in 1149 days
Open ports: 9443
Found by BigIPVersion

Laos SkytelecomTransit provider and ISP in Vientiene. 2022-05-29 18:01 2025-07-22 02:09
cf2af256dac5ffc3a76f424dcc3822870550078e0550078e0550078e0550078e
https://202.123.176.101:9443

```
Found BIG IP: BIG-IP® - F5_2.edl.com (10.0.100.18)
Year 2018
Vulnerable to CVE-2022-1388
```

[redacted]
critical
> BIG-IP®- Redirect
ASN: 4808
110 events in 248 days
Open ports: 443
[redacted]

China China Unicom Beijing Province Network 2024-11-15 19:15 2025-07-22 01:06
cf2af256dac5ffc3415b83d7813b58d23639fad13639fad13639fad13639fad1
https://123.127.164.61

```
Found BIG IP: BIG-IP® - CARLC2.com (127.0.0.1)
Year 2017
Vulnerable to CVE-2022-1388
```

[redacted]
critical
> BIG-IP®- Redirect
ASN: 201771
46 events in 89 days

Saudi Arabia Arabian Internet & Communications Services Co.ltd 2025-04-23 02:46 2025-07-21 23:15
cf2af256dac5ffc3a709dd19041655ac65150f6365150f6365150f6365150f63
https://95.177.178.89

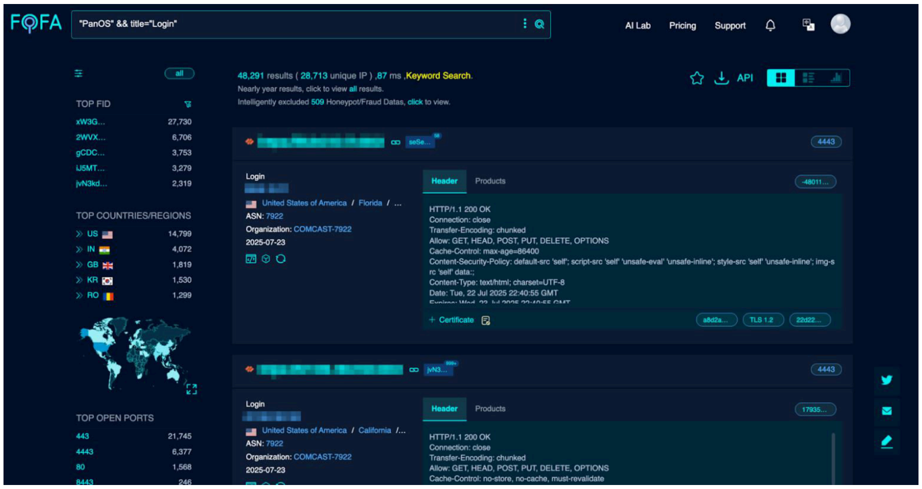
```
Found BIG IP: BIG-IP® - f5waf-33202.bluvalt.com (10.10.7.3)
Year 2017
```

Attack Case Study: PAN-OS

For this attack, Miyako found a completely prepackaged and ready-to-go multi-CVE PoC GitHub. Similar to the telecommunications company example, Miyako used a search engine to identify victims. However, this time they used FOFA, searching for organizations running PAN-OS that also have VPNs exposed to the internet.

This allowed them to:

- Filter by country, port, or organization
- Export the list of exposed logins
- Weaponize the list



"PanOS" && title="Login"

48,291 results (28,713 unique IP) ,87 ms ,Keyword Search.
Nearly year results, click to view all results.
Intelligently excluded 509 Honeypot/Fraud Datas, click to view.

TOP FID	
xW3G...	27,730
2WVX...	6,706
gCDC...	3,753
iJ5MT...	3,279
jvN3kd...	2,319

TOP COUNTRIES/REGIONS	
US	14,799
IN	4,072
GB	1,819
KR	1,530
RO	1,299

TOP OPEN PORTS	
443	21,745
4443	6,377
80	1,568
8443	246

[redacted] seSe... 58 4443

Login
[redacted]
United States of America / Florida / ...
ASN: 7922
Organization: COMCAST-7922
2025-07-23

-48011...

```
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
Cache-Control: max-age=86400
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-s
rc 'self' data:;
Content-Type: text/html; charset=UTF-8
Date: Tue, 22 Jul 2025 22:40:55 GMT
```

a8d2a... TLS 1.2 22d22...

[redacted] jvN3... 999+ 4443

Login
[redacted]
United States of America / California /...
ASN: 7922
Organization: COMCAST-7922
2025-07-23

17935...

```
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
Cache-Control: no-store, no-cache, must-revalidate
```

Key Takeaway for Security Teams: Open-Source Research is for Everyone (Including Threat Actors)

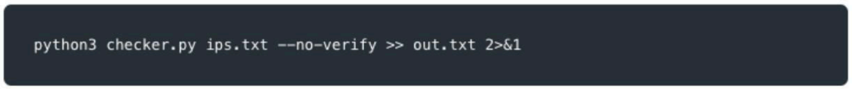
Everything that legitimate security teams can access, threat actors can access too. Malicious actors actively weaponize PoCs because they know the exploits can work without investing time, effort, or technology resources. As soon as researchers click publish, the vulnerability can quickly move along the Common Vulnerability Scoring System (CVSS) “PoC available” to “active exploitation.”

Common Tactic #3: Automate Activities

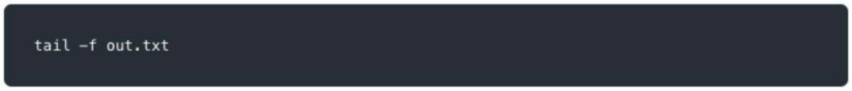
Financially motivated threat actors want to target as much important data as possible with as little effort as possible. They can streamline their operations with automation, just like legitimate businesses.

Attack Case Study: PAN-OS

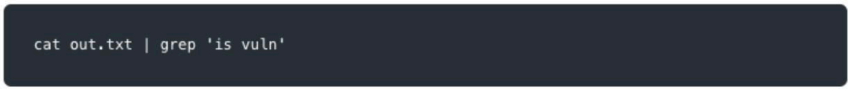
To automate this attack, Hellcat exported the list of IP addresses from the FOFA search and saved that as a text file. Then, they made a custom checker script in Python to run through the PoC and exploit it to a text file. They automated the process so they could achieve remote code execution for any companies with vulnerable live hosts.



```
python3 checker.py ips.txt --no-verify >> out.txt 2>&1
```



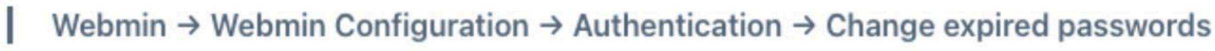
```
tail -f out.txt
```



```
cat out.txt | grep 'is vuln'
```

Attack Case Study: Government Server

In this case, Miyako leveraged two different types of automation. Initially, they used Python to create a checker that identified the infrastructure and vulnerable servers. After finding that the Firebird databases had default passwords, they were able to use automation for brute forcing access. Instead of spending the time and resources to create zero day attacks, they automated the breaches.



> Webmin → Webmin Configuration → Authentication → Change expired passwords

Key Takeaway for Security Teams: Automation Makes Attacks More Lucrative

Threat actors treat data breaches like a business:

- They monitor their return on investment and work to reduce operational costs.
- They automate as many attack processes as possible.

Malicious actors across skill levels will look for ways to make fast money, especially when an organization's infrastructure makes the process easy.

Lessons Learned: Any Barrier is Risk Mitigation

When security professionals say "think like a cybercriminal," they increasingly mean "think like a business person." As financially motivated threat actors want quick attacks that earn a high income, any digital roadblock becomes a deterrent.

According to the Hellcat manual, most attacks are crimes of opportunity rather than targeted attacks. They stumble upon vulnerable infrastructure, identify the valuable assets, and exfiltrate data to any location that looks "normal," like a Dropbox or Google Drive (as opposed to an obscure IP address which may immediately seem more suspicious).

Organizations that want to mitigate data breach risks can put up barriers that reduce a cyber attack's ROI, even with "simple" activities like:

- Changing default passwords
- Implementing multi-factor authentications
    - To protect against MFA fatigue attacks, train employees to be aware of this attack method, and also protect session cookies
- Patching vulnerabilities as quickly as possible, especially if a PoC is available
- Monitoring network traffic to detect malicious listeners, beacons, and implants
- Monitoring for cron jobs that threat actors use to gain a temporary foothold
- Monitoring for new or hijacked services, like fake-but-legitimate looking system services or replaced services like sshd
- Implementing data leak prevention software or firewall management to identify any large amounts of data that is going outside of the organization

Threat Exposure Management with Flare

The Flare Threat Exposure Management solution empowers organizations to proactively detect, prioritize, and mitigate the types of exposures commonly exploited by threat actors. Our platform automatically scans the clear & dark web and prominent threat actor communities 24/7 to discover unknown events, prioritize risks, and deliver actionable intelligence you can use instantly to improve security.

Flare integrates into your security program in 30 minutes and often replaces several SaaS and open source tools. See what external threats are exposed for your organization by signing up for our free trial.

Gartner Peer Insights
4.9 ★★★★★

AICPA
SOC 2
TYPE II
Thoropass™

Sign Up for a Free Trial →

flare

flare.io

hello@flare.io