RAPID7

Into the Wild: Exploring Today’s Top Threats

Ken Mizota
Chief Technology Officer, APJ

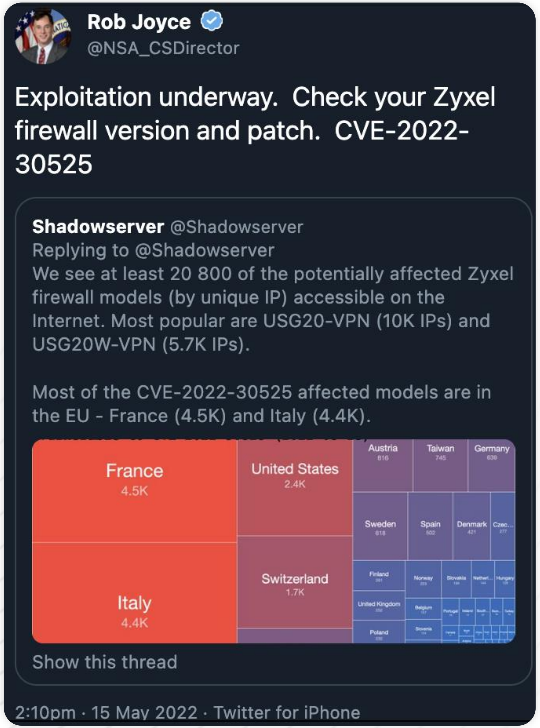
Speakers

Ken Mizota

CTO Asia-Pacific & Japan

Rapid7 researchers analyze thousands of vulnerabilities each year to understand root causes, dispel misconceptions and share information on exploitability.

Identifying threats - the reality



Rob Joyce @NSA_CSDirector

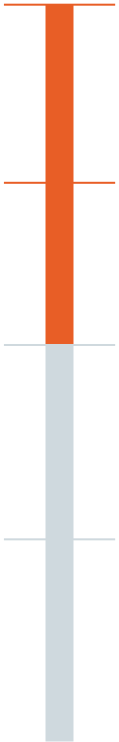
Exploitation underway. Check your Zyxel firewall version and patch. CVE-2022-30525

Shadowserver @Shadowserver
Replying to @Shadowserver
We see at least 20 800 of the potentially affected Zyxel firewall models (by unique IP) accessible on the Internet. Most popular are USG20-VPN (10K IPs) and USG20W-VPN (5.7K IPs).

Most of the CVE-2022-30525 affected models are in the EU - France (4.5K) and Italy (4.4K).

Show this thread

2:10pm · 15 May 2022 · Twitter for iPhone



April 13

Disclosure

Rapid7 makes the disclosure to Zyxel, who acknowledges on April 14, 2022.

April 28

Patches made available

Zyxel releases patches silently without coordinating with Rapid7.

May 9

We notice the patches are available

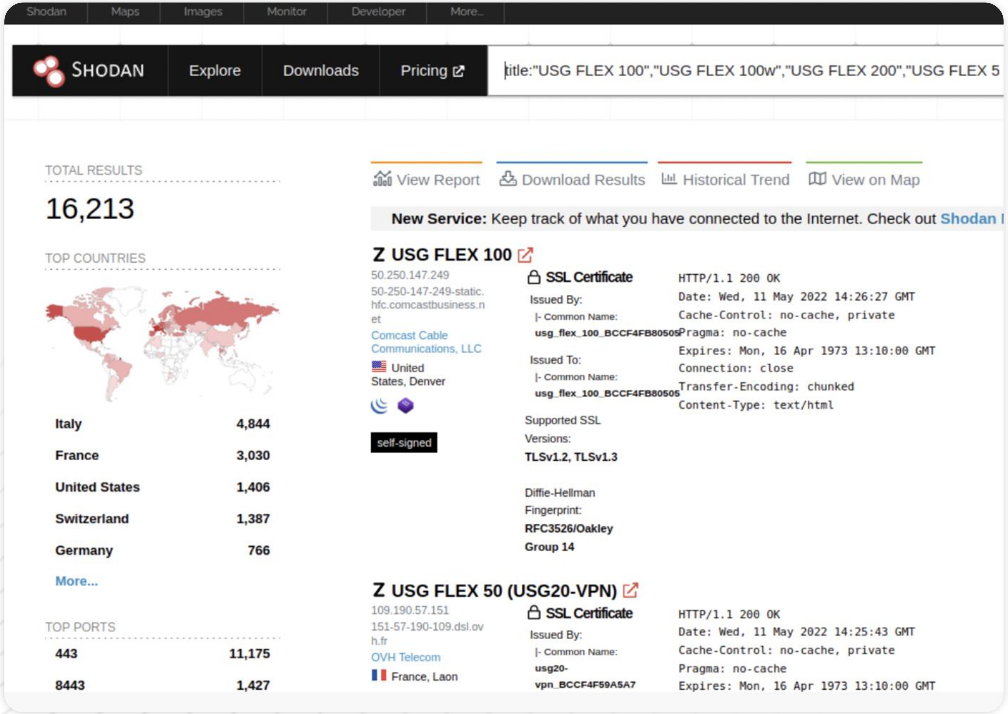
Rapid7 asks Zyxel for a response on the silent patches and indicates we will disclose the week of May 9, 2022. Research team publishes their disclosure May 12.

May 15

Someone I follow posted it on Twitter

I read the tweet and dig into the vulnerability

Sound the alarm….



title:"USG FLEX 100","USG FLEX 100w","USG FLEX 200","USG FLEX 5

TOTAL RESULTS

16,213

TOP COUNTRIES

Italy	4,844
France	3,030
United States	1,406
Switzerland	1,387
Germany	766

More...

TOP PORTS

443	11,175
8443	1,427

New Service: Keep track of what you have connected to the Internet. Check out Shodan

USG FLEX 100

50.250.147.249
50-250-147-249-static.hfc.comcastbusiness.net
Comcast Cable Communications, LLC
United States, Denver

SSL Certificate
Issued By:
|- Common Name:
usg_flex_100_BCCF4FB80505
Issued To:
|- Common Name:
usg_flex_100_BCCF4FB80505
Supported SSL Versions:
TLSv1.2, TLSv1.3
Diffie-Hellman Fingerprint:
RFC3526/Oakley Group 14

```
HTTP/1.1 200 OK
Date: Wed, 11 May 2022 14:26:27 GMT
Cache-Control: no-cache, private
Pragma: no-cache
Expires: Mon, 16 Apr 1973 13:10:00 GMT
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html
```

USG FLEX 50 (USG20-VPN)

109.190.57.151
151-57-190-109.dsl.ovh.fr
OVH Telecom
France, Laon

SSL Certificate
Issued By:
|- Common Name:
usg20-vpn_BCCF4F59A5A7

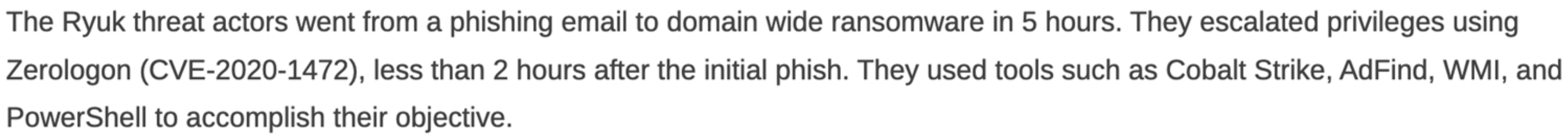
```
HTTP/1.1 200 OK
Date: Wed, 11 May 2022 14:25:43 GMT
Cache-Control: no-cache, private
Pragma: no-cache
Expires: Mon, 16 Apr 1973 13:10:00 GMT
```

Affected Model	Affected Firmware Version
USG FLEX 100, 100W, 200, 500, 700	ZLD5.00 thru ZLD5.21 Patch 1
USG20-VPN, USG20W-VPN	ZLD5.10 thru ZLD5.21 Patch 1
ATP 100, 200, 500, 700, 800	ZLD5.10 thru ZLD5.21 Patch 1

What exactly is this vuln, and am I covered?

- Vulnerabilities discovered by Rapid7's Emergent Threat Response (ETR) Team
- Unauthenticated RCE on Zyxel Firewalls, leveraging a command injection within an HTTP POST request
- Affects Zyxel firewalls with zero touch provisioning

You had a password of Welcome…



The Ryuk threat actors went from a phishing email to domain wide ransomware in 5 hours. They escalated privileges using Zerologon (CVE-2020-1472), less than 2 hours after the initial phish. They used tools such as Cobalt Strike, AdFind, WMI, and PowerShell to accomplish their objective.

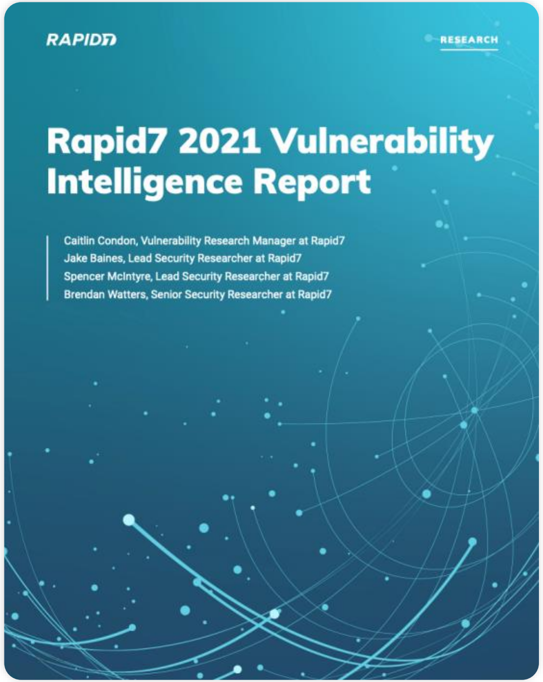
Source: DFIR Report

Vulnerability Intelligence for Today’s Threat Landscape

Rapid7 researchers analyze thousands of vulnerabilities each year to understand root causes, dispel misconceptions, and share information on exploitability.

Annual Vulnerability Intelligence Report:

- 50 high-priority threats that pose risk to organisations of all sizes
- Notable attack vectors
- Attack analysis that helps you predict and prioritise action



RAPID7

RESEARCH

Rapid7 2021 Vulnerability Intelligence Report

Caitlin Condon, Vulnerability Research Manager at Rapid7
Jake Baines, Lead Security Researcher at Rapid7
Spencer McIntyre, Lead Security Researcher at Rapid7
Brendan Watters, Senior Security Researcher at Rapid7

Threat Status

🟧 **Widespread Threat**

A vulnerability that is exploited by many attackers across many different industries and organisations.

⬛ **Threat**

A vulnerability that has been reported as exploited in the wild by reputable sources, including Rapid7's own Labs and services teams.

◼ **Impending Threat**

A vulnerability that has not seen exploitation by adversaries, but in our view, is a likely and valuable attack target.

Current Threat Landscape

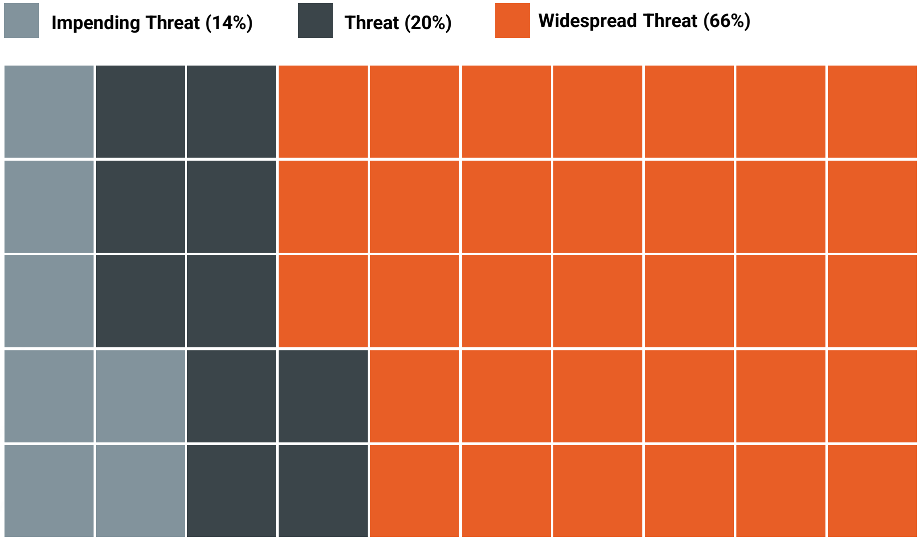
Dramatic increase in widespread attacks (136%)

- Many attackers, many targets
- Rise of “attacker economies of scale”
- 64% of widespread threat vulnerabilities were used in ransomware operations

Unprecedented rise in zero-day attacks

- More than half of widespread threats began with a zero-day exploit
- Red flag for conventional patch cycles, development of emergency protocols

2021 Vulnerability by Threat Status

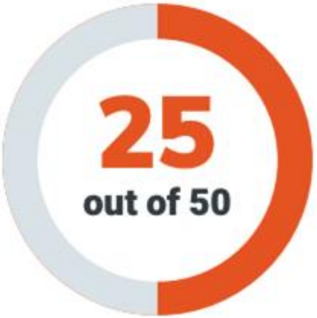


71% decrease in time to known exploitation (TTKE)

Time to Known Exploitation (TTKE)

- Time between when a vulnerability becomes known and when it is used in the wild by adversaries
- Based on primary disclosure sources (vendor advisories, code repositories, open intel)
- Average time between disclosure and exploitation dropped from 42 days (2020) to **12 days** (2021)
- Driven largely by rise in zero-day exploitation
- Significant implications for security and IT teams

2021



in report were exploited within

7 days of disclosure

Vulnerability Class and Threat Status

Improper Access Control

Typically indicate a missing requirement e.g. authentication or configured to be overly permissive when security controls should restrict access.

Deserialization

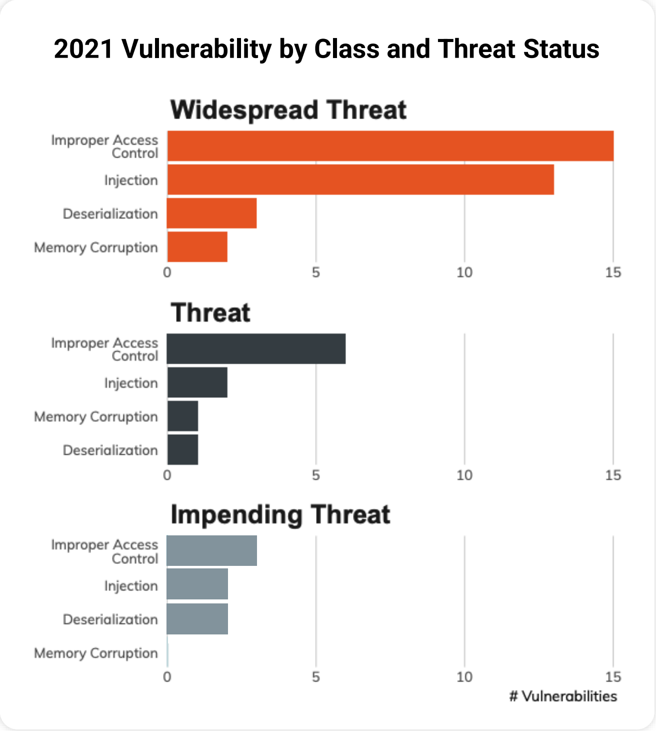
Blobs of data that are wrapped in code and can be executed by surprise. Reputation for high exploitability and many off-the-shelf tools to build exploit chains.

Injection

Use specially crafted input and techniques to compromise data integrity or run arbitrary code as a high-privileged user

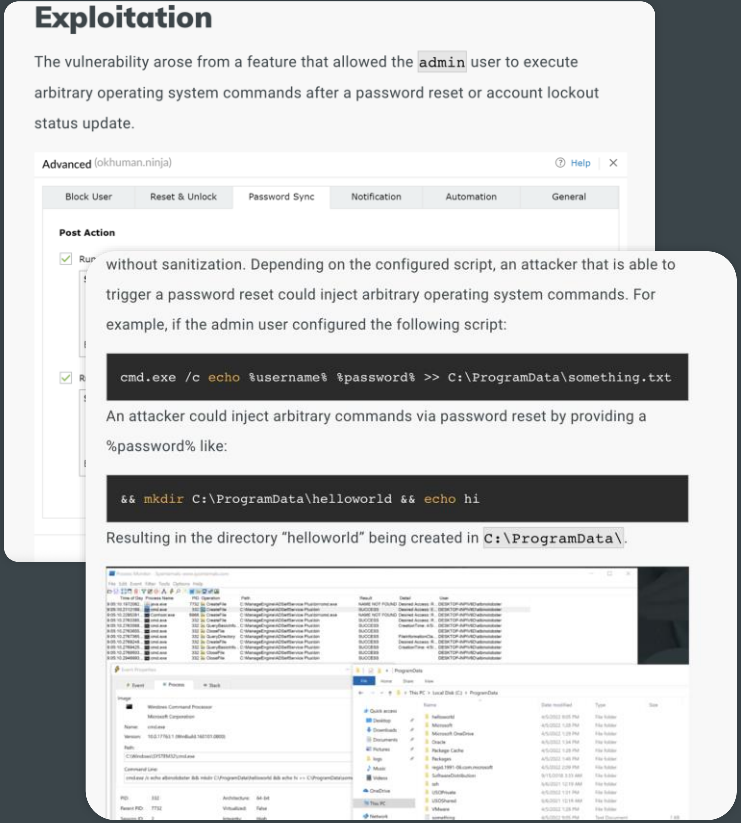
Memory Corruption

A misalignment of assumptions between a network or file protocol and the CPU; difficult to exploit reliably at scale, but often used in targeted attacks by sophisticated threat actors. Common in zero-day attacks on things like browsers.



Zero-Day Exploitation of Zoho ManageEngine ADSelfService Plus

- Rapid7 Managed Detection and Response (MDR) team discovered a threat campaign targeting ManageEngine ADSelfService Plus
- Custom scripts feature exploited by remote attackers with valid admin credentials
- Rapid7 vulnerability researchers wrote an exploit to mimic the zero-day attack
- Vendor assigned CVE-2022-28810, patched within three days
- Assess exposure with InsightVM, test security controls with Metasploit, detect attacks with InsightIDR



Exploitation

The vulnerability arose from a feature that allowed the `admin` user to execute arbitrary operating system commands after a password reset or account lockout status update.

without sanitization. Depending on the configured script, an attacker that is able to trigger a password reset could inject arbitrary operating system commands. For example, if the admin user configured the following script:

```
cmd.exe /c echo %username% %password% >> C:\ProgramData\something.txt
```

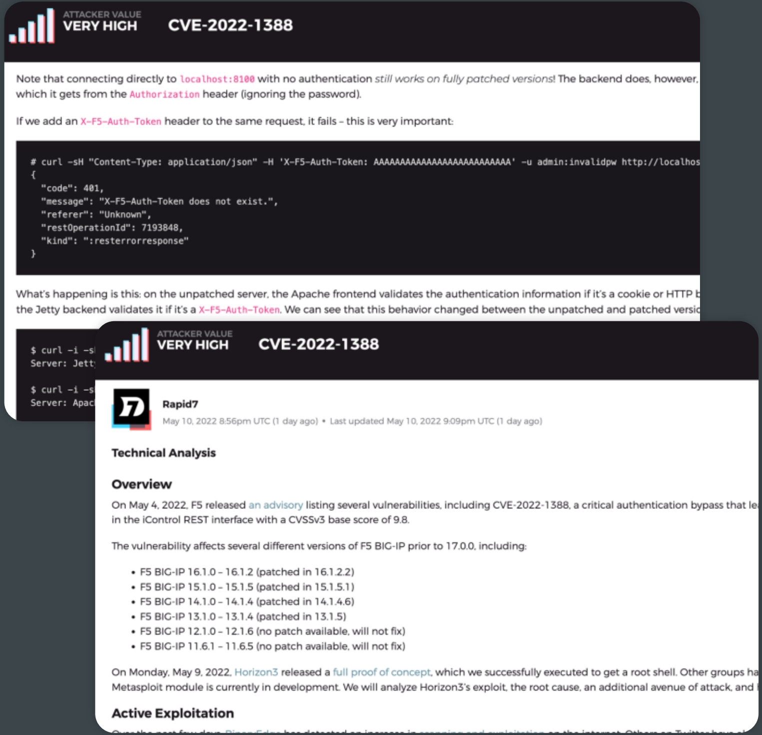
An attacker could inject arbitrary commands via password reset by providing a %password% like:

```
&& mkdir C:\ProgramData\helloworld && echo hi
```

Resulting in the directory "helloworld" being created in `C:\ProgramData\`.

CVE-2022-1388: F5 BIG-IP Authentication Bypass RCE

- Network edge, trivially exploitable
- Rapid7 analysis of root cause, exploitation, and attack vectors
- Time to known exploitation = 5 days
- 2,500 internet-facing targets, more beneath the surface
- Search `/var/log/audit` for commands executed by `icrd_child`
- Assess exposure with InsightVM and Nexpose, test security controls with Metasploit



ATTACKER VALUE
VERY HIGH
CVE-2022-1388

Note that connecting directly to `localhost:8100` with no authentication *still works on fully patched versions*! The backend does, however,
which it gets from the `Authorization` header (ignoring the password).

If we add an `X-F5-Auth-Token` header to the same request, it fails – this is very important:

```
# curl -sH "Content-Type: application/json" -H 'X-F5-Auth-Token: AAAAAAAAAAAAAAAAAAAAAAAAAA' -u admin:invalidpw http://localhos
{
  "code": 401,
  "message": "X-F5-Auth-Token does not exist.",
  "referer": "Unknown",
  "restOperationId": 7193848,
  "kind": ":resterrorresponse"
}
```

What's happening is this: on the unpatched server, the Apache frontend validates the authentication information if it's a cookie or HTTP b
the Jetty backend validates it if it's a `X-F5-Auth-Token`. We can see that this behavior changed between the unpatched and patched versic

```
$ curl -i -s
Server: Jetty

$ curl -i -s
Server: Apac
```

ATTACKER VALUE
VERY HIGH
CVE-2022-1388

Rapid7
May 10, 2022 8:56pm UTC (1 day ago) • Last updated May 10, 2022 9:09pm UTC (1 day ago)

Technical Analysis

Overview

On May 4, 2022, F5 released an advisory listing several vulnerabilities, including CVE-2022-1388, a critical authentication bypass that le
in the iControl REST interface with a CVSSv3 base score of 9.8.

The vulnerability affects several different versions of F5 BIG-IP prior to 17.0.0, including:

- F5 BIG-IP 16.1.0 – 16.1.2 (patched in 16.1.2.2)
- F5 BIG-IP 15.1.0 – 15.1.5 (patched in 15.1.5.1)
- F5 BIG-IP 14.1.0 – 14.1.4 (patched in 14.1.4.6)
- F5 BIG-IP 13.1.0 – 13.1.4 (patched in 13.1.5)
- F5 BIG-IP 12.1.0 – 12.1.6 (no patch available, will not fix)
- F5 BIG-IP 11.6.1 – 11.6.5 (no patch available, will not fix)

On Monday, May 9, 2022, Horizon3 released a full proof of concept, which we successfully executed to get a root shell. Other groups ha
Metasploit module is currently in development. We will analyze Horizon3's exploit, the root cause, an additional avenue of attack, and

Active Exploitation

Prioritisation

2,100,000

7.9

Risk scoring

Risk Score
2.0

@InsightVM

Understand what compensating controls exist within the environment.

@Metasploit

Understand the vulnerability, determine likely impact

@ThreatConnect

Is the vulnerability being exploited?
Targeting my geo/industry

What does this mean for my organisation?

- Patch vulnerabilities used in widespread attacks. If you haven’t done so already, prioritise remediation for the highlighted vulnerabilities from 2021 and 2022.

- Know where your exposed and likely targets sit. Attackers home in on commonly exposed technologies (think VPNs and remote access gateways). vCenter Server or similar critical network infrastructure systems should be a high priority every time.

- Asset management is everything. Knowledge of, and responsibility for, the assets on the network go hand-in-hand. Scan everything, all the time, inside and out.

- Patch cycles and patch exceptions: Build in exceptions to your patching program today. Exceptional patching is becoming the low bar, and presumes "normal" patching. You can’t up-level to effective emergency procedures without a strong “normal” VM foundation.

- Risk tolerance: It's okay to have risky systems, as long as that risk is articulated and accepted. Understanding vulnerability profiles can make risk calculations easier to understand and communicate.

Resources

https://www.rapid7.com/info/2021-vulnerability-intelligence-report/

- Full vulnerability dataset available at the end of the report, including threat status, attacker utility, vulnerability class, and time to known exploitation
- Most CVEs linked to technical analyses from our vuln research teams

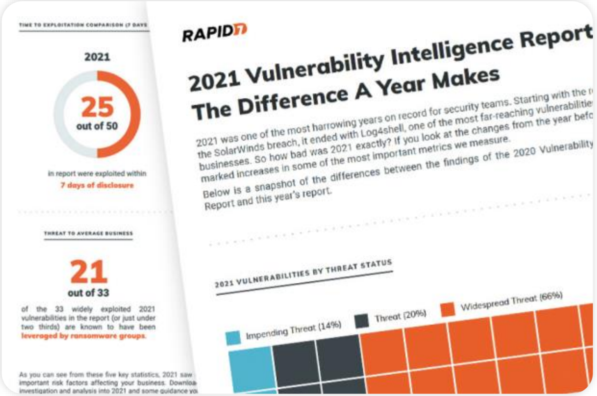
https://attackerkb.com/

- In-depth exploitability analysis for active and impending threats

https://blog.rapid7.com/tag/emergent-threat-response/

- "What you need to know" synopses of critical vulnerabilities

Twitter: @Rapid7, @Metasploit, @kenmizota



TIME TO EXPLOITATION COMPARISON (7 DAYS

2021

25
out of 50

in report were exploited within
7 days of disclosure

THREAT TO AVERAGE BUSINESS

21
out of 33

of the 33 widely exploited 2021 vulnerabilities in the report (or just under two thirds) are known to have been leveraged by ransomware groups.

As you can see from these five key statistics, 2021 saw
important risk factors affecting your business. Downloa
investigation and analysis into 2021 and some guidance yo

RAPID7

2021 Vulnerability Intelligence Report
The Difference A Year Makes

2021 was one of the most harrowing years on record for security teams. Starting with the
the SolarWinds breach, it ended with Log4shell, one of the most far-reaching vulnerabilitie
businesses. So how bad was 2021 exactly? If you look at the changes from the year befo
marked increases in some of the most important metrics we measure.

Below is a snapshot of the differences between the findings of the 2020 Vulnerability
Report and this year's report.

2021 VULNERABILITIES BY THREAT STATUS