

Building Defensive Playbooks from Others Misfortune

Chester Wisniewski
Principal Research Scientist

September 2022

SOPHOS

Why am I qualified to give this talk

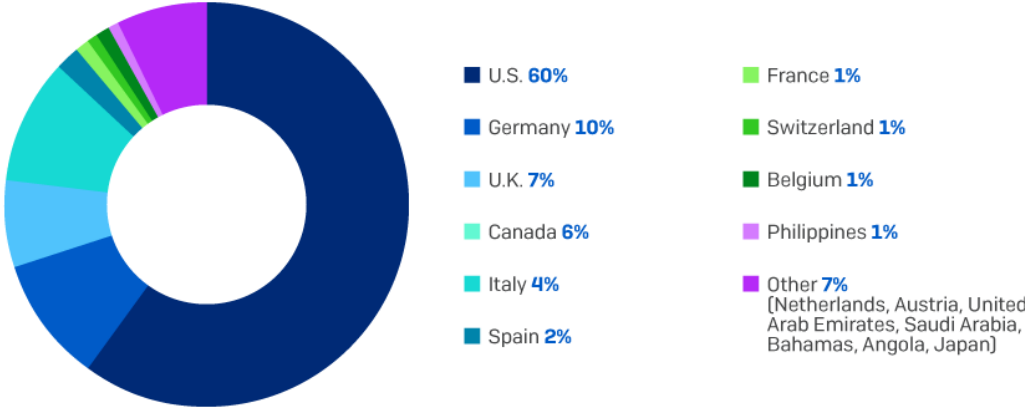
- 19 years at Sophos, 25 in security
- Liasson with Sophos Researchers (200+) on latest threats, tricks, and tactics
- Access to threat intelligence gathered from more than 500,000 organizations in 150 countries
- Participate in the InfoSec community at conferences and through Twitter to learn the latest TTPs
- Have presented original research at RSA Conference, BSides, Virus Bulletin, Cloud Expo Asia and more



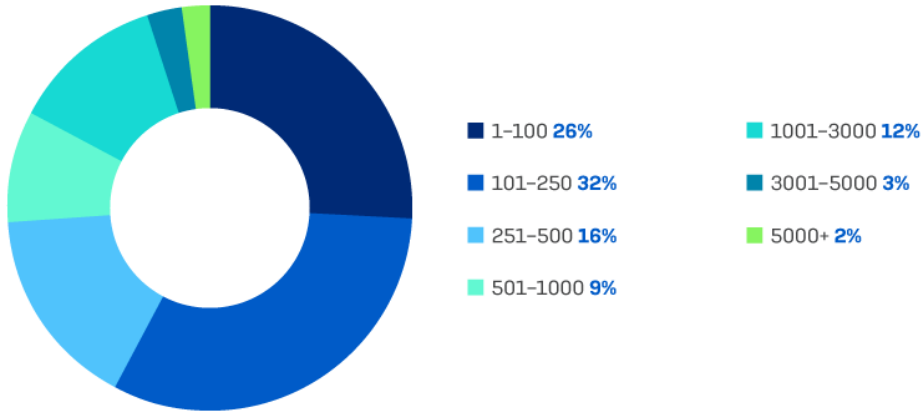
Demographic Profile of Active Adversary Playbook sources

144 incidents
 17 countries
 Multiple sectors

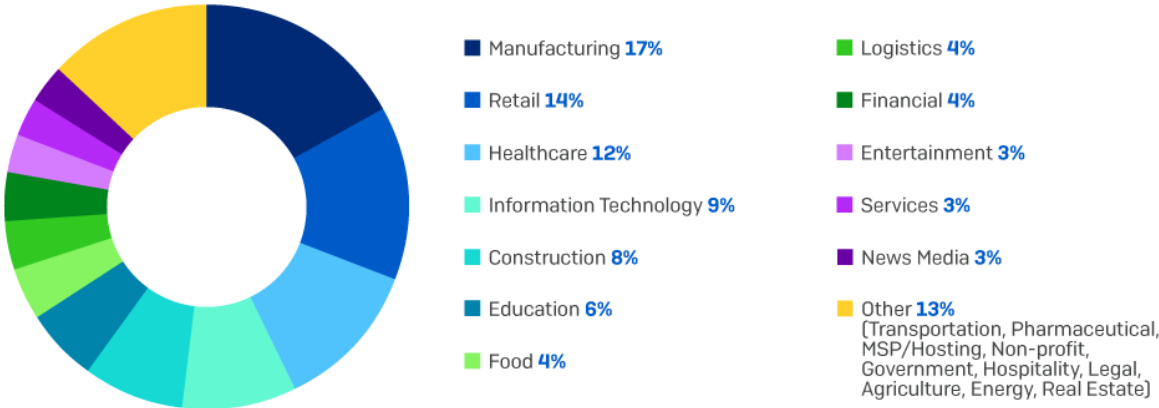
Incident Response Cases by Country



Incident Response Cases by Organization Size (Number of Employees)

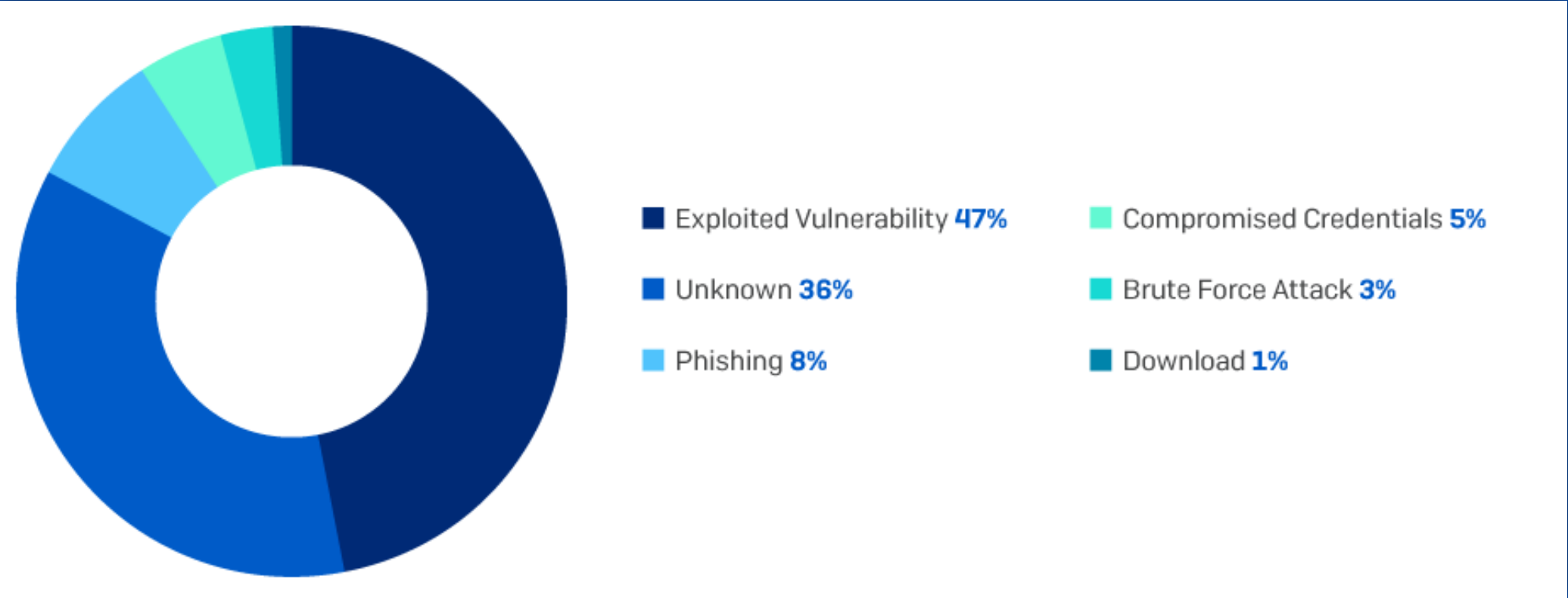


Incident Response Cases by Sector

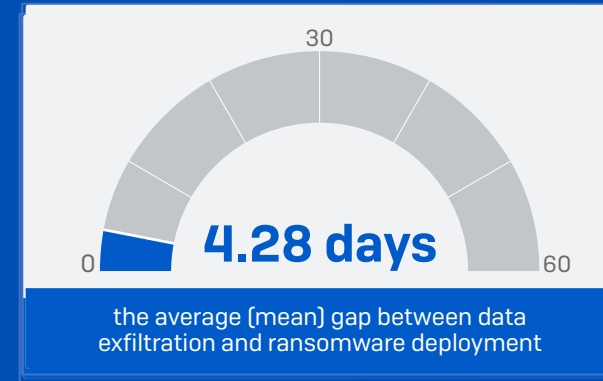
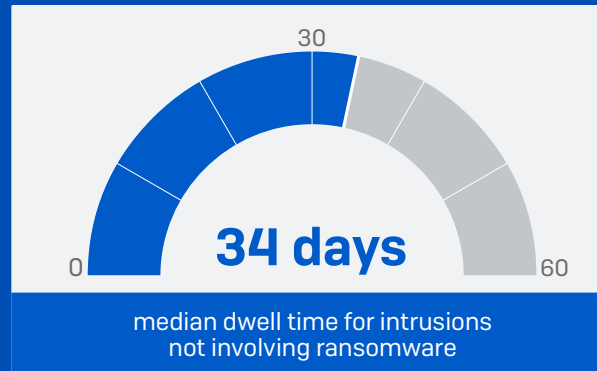
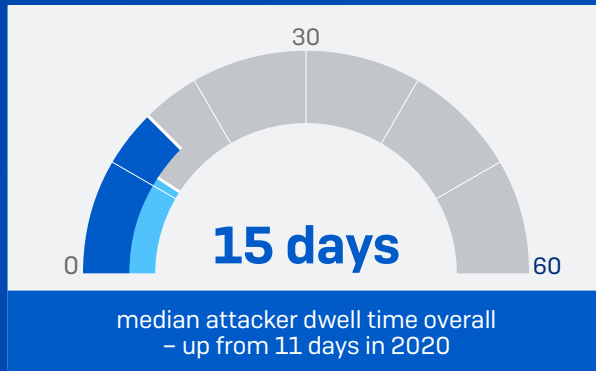


How we fail

Root Causes of Attacks in 2021



Intruder Dwell Time

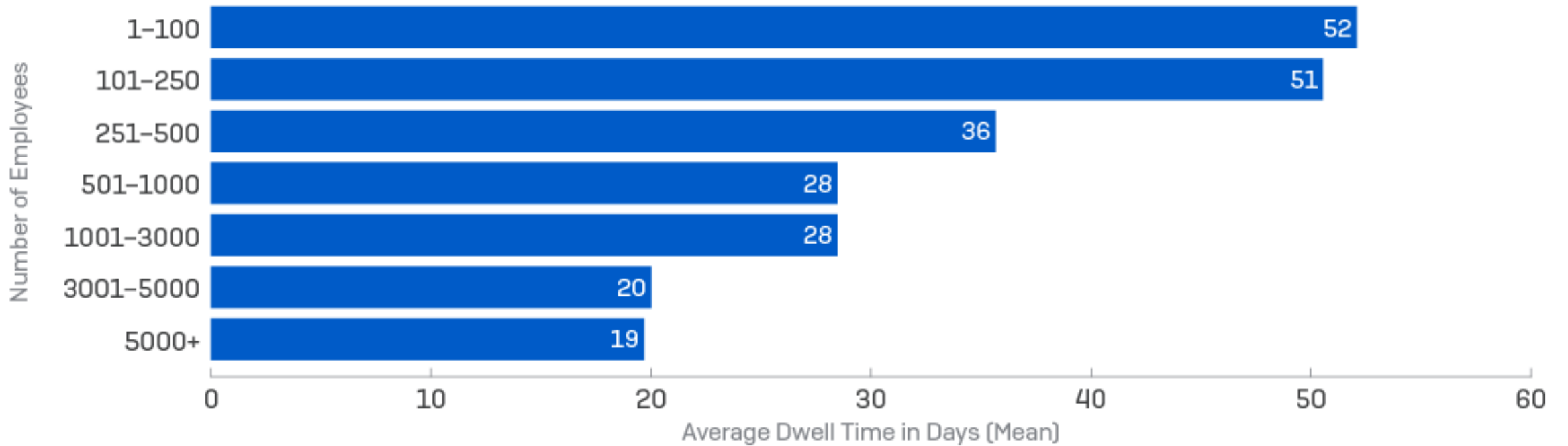


Variations in Average Intruder Dwell Time (Median)




Smaller Business Experienced Longer Dwell Times

Intruder Dwell Time by Company Size (Mean)



Why is dwell time so high and variable!?


UAS RDP SHOP #1

SKY-FRAUD.RU

News
FAQ
RDP
SSN
History ▾
Billing
Tickets
Settings
Logout

ajohnson
\$ 0.00
🇺🇸 English

UPDATE RDP !!!

UPDATE RDP !!!

ADDED 2600 NEW RDP !!!
ADDED 1100 RESSEL RDP !!!

Now you're able to check IP address before purchase a server. The price for service is \$0.30. You can check 5 IP address (checked 5 IP's you have to buy any server to continue checking). The service is available only for users that already made

NEW BONUS PROGRAM BY UAS! ADD TO YOUR ACCOUNT 1000 USD BY TOPUP AND YOU RECEIVE 1100 USD TO YOUR information - contact us at JID: UAS-Admin@hack-jabb.ru

SSN (Social Security Number) - Very Very Fresh!

Price for items with year of birth till 1970 - \$1
Price for items with year of birth from 1970 and higher - \$2

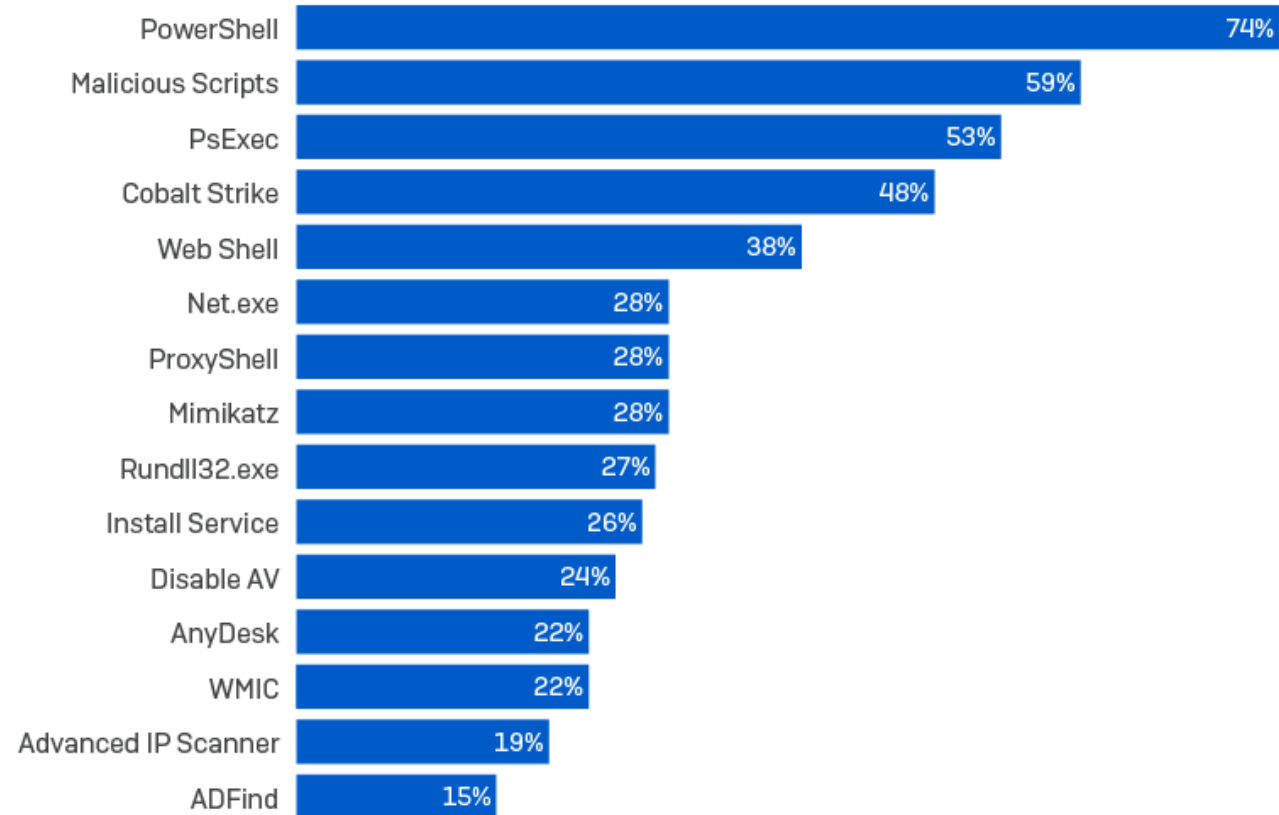
TUNE UP YOUR ANONYMITY FROM GOOD TO BEST LEVEL RIGHT NOW !!! ENJOY !!!

Total found: 16011
Показать: 50 ▾

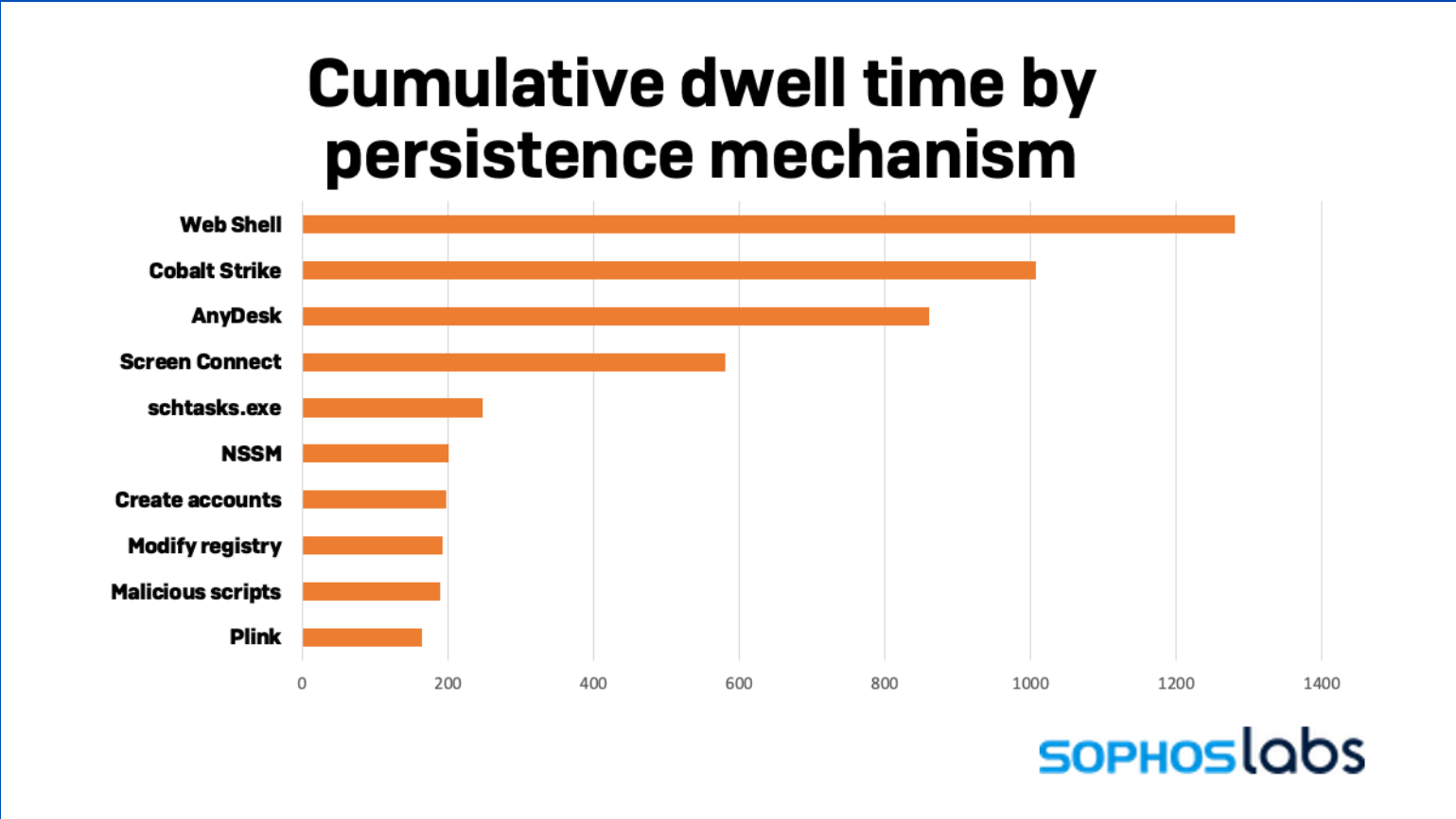
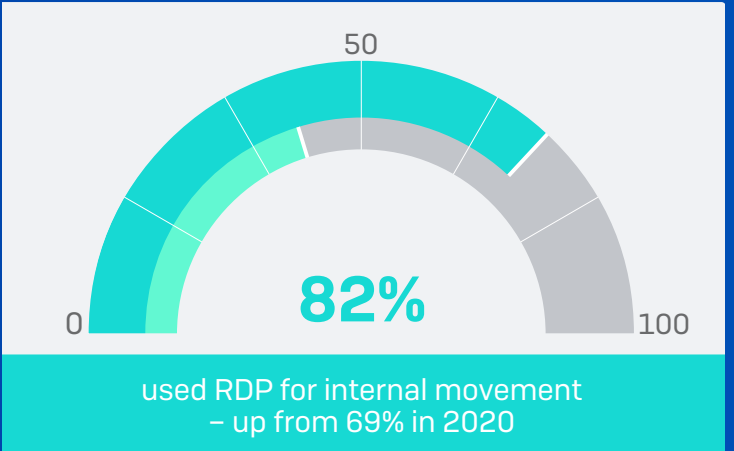
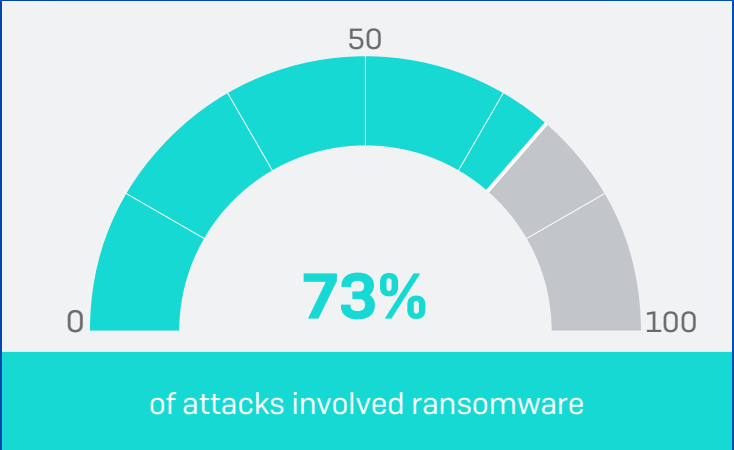
IP	Country	State	City	ZIP	OS	RAM	Dwn.	Upl.	Direct IP	Admin Rights	Added	Price, \$
86.**.*	🇭🇺 HU	Budapest	Budapest	1092	Windows 7 Professional	6 GB	5.56 Mbit/s	3.89 Mbit/s			add funds!	13.00
45.**.* - Vultr	🇬🇧 GB	England	Spitalfields	E1	Windows 10 Pro	1 GB	6.27 Mbit/s	4.39 Mbit/s		✓	add funds!	11.00
103.**.*	🇮🇳 IN	Maharashtra	Mumbai	400099	Windows 7 Professional	--	8.64 Mbit/s	6.05 Mbit/s			add funds!	12.00
134.**.*	🇫🇷 FR	Grand-Est	Strasbourg	67999	Windows Server 2012 R2 Standard	1 GB	4.57 Mbit/s	3.20 Mbit/s		✓	add funds!	16.00
18.**.* - AWS	🇺🇸 US	Ohio	Columbus	43085	Windows Server 2019 Datacenter	1 GB	4.84 Mbit/s	3.39 Mbit/s		✓	add funds!	10.00
103.**.*	🇨🇳 HK	Hong Kong	Hong Kong	-	Windows 7 Professional	--	10.57 Mbit/s	7.40 Mbit/s		✓	add funds!	19.00
46.**.*	🇬🇧 GB	England	Leeds	ME17	Windows Server 2008 R2 Standard	1 GB	11.57 Mbit/s	8.10 Mbit/s	✓		add funds!	13.00
210.**.*	🇰🇷 KR	Seoul-teukbyeolsi	Seoul	06030	Windows Server (R) 2008 Standard	--	9.28 Mbit/s	6.50 Mbit/s	✓		add funds!	15.00
39.**.*	🇨🇳 CN	Zhejiang	Hangzhou	310099	Windows Server 2008 R2 Enterprise	--	9.28 Mbit/s	6.50 Mbit/s		✓	add funds!	16.00
192.**.*	🇺🇸 US	California	La Jolla	92037	Windows Server 2016 Standard	4 GB	10.51 Mbit/s	7.36 Mbit/s		✓	add funds!	17.00
132.**.*	🇵🇾 PY	Alto Parana	Ciudad del Este	7000	Windows Server 2016 Standard	--	5.32 Mbit/s	3.72 Mbit/s			add funds!	16.00
45.**.* - Vultr	🇩🇪 DE	Hessen	Frankfurt am Main	65931	Windows 10 Pro	1 GB	8.21 Mbit/s	5.75 Mbit/s	✓	✓	add funds!	15.00

Legitimate tools increase stealth

2021

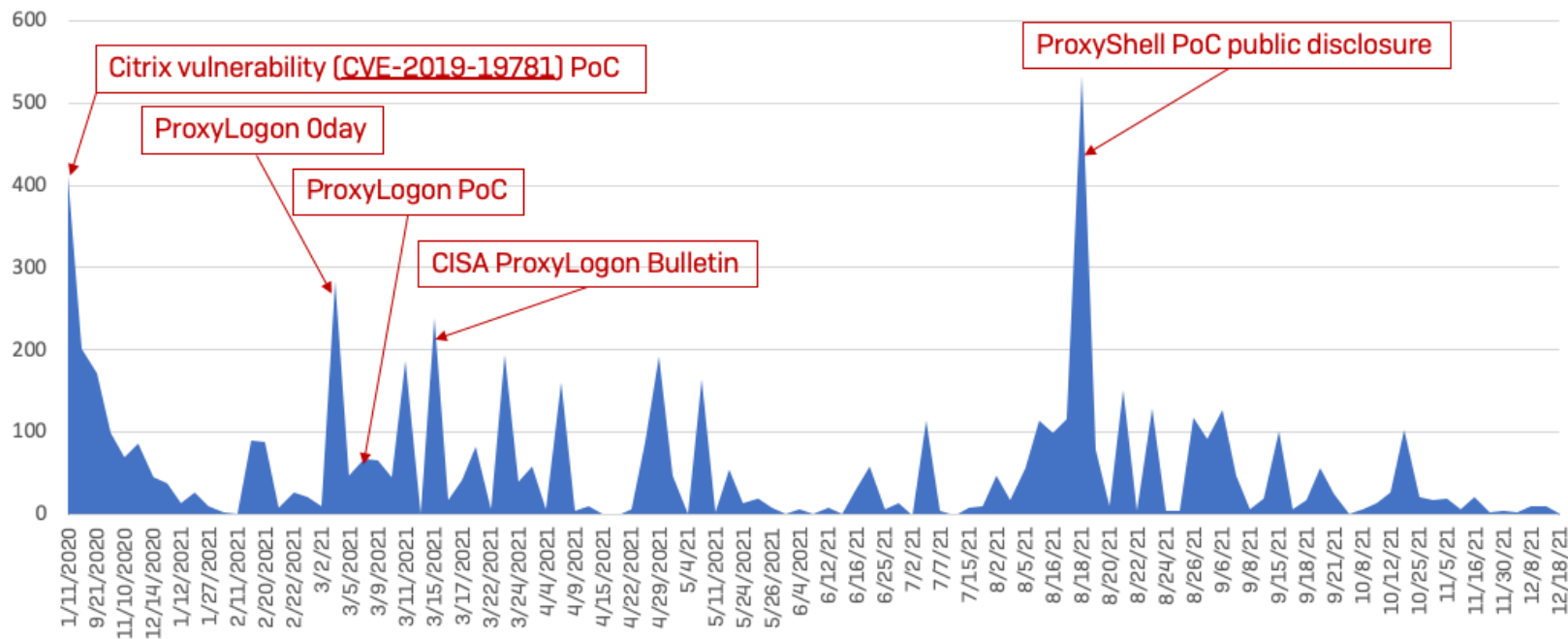


Other indicators from our study



Most abused vulnerabilities and infection times

Cumulative dwell time of intrusions by intrusion start date



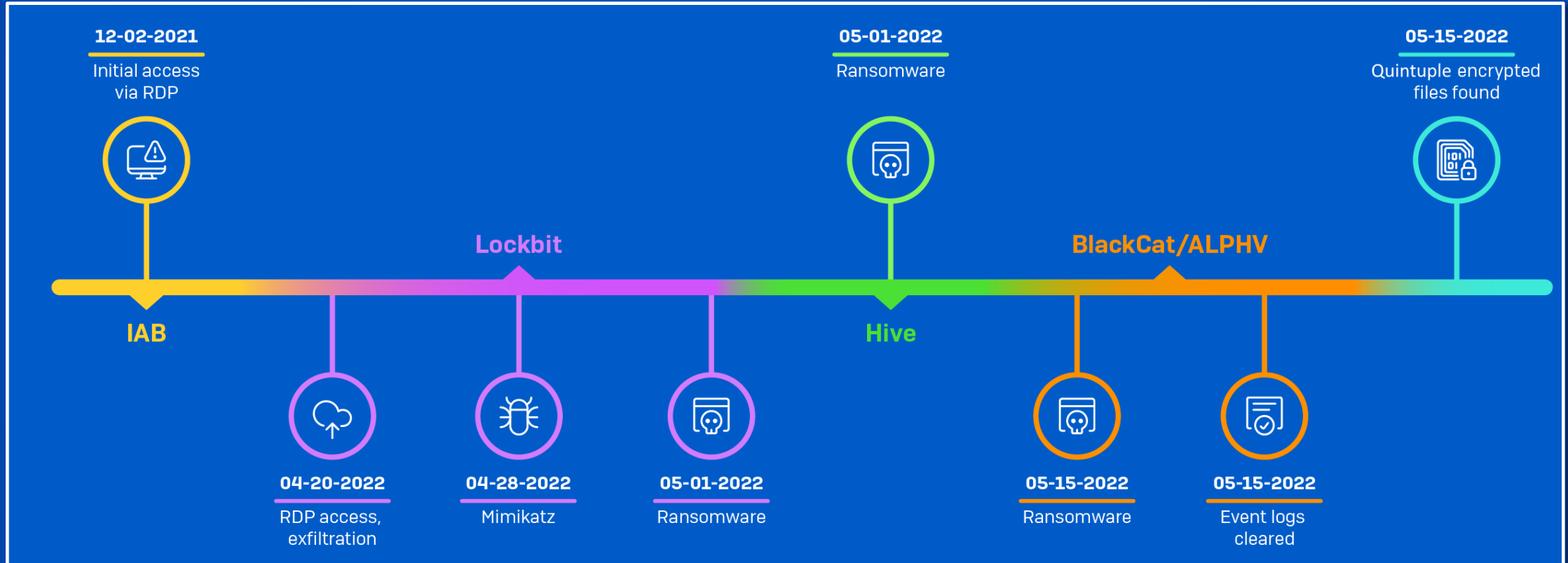
SOPHOSlabs

Exfiltration



- Finance
- HR
- IT
- Budgets
- Legal
- Password spreadsheets/lists

Exclusivity? Not so much



Lockbit, Hive and BlackCat attack automotive supplier in triple ransomware attack

What to do?

Patching our priorities

- Patching never more important
- CISA Known Exploited Vulns (KEV) list
- Servers, infrastructure, then endpoints
- Everything, but in order
- Security vs. IT
- Not all systems are equal

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE S

ADVISORY —

Feds say hackers are likely exploiting critical Fortinet VPN vulnerabilities

Exploits allow hackers to log into VPNs and then access


DAN GOODIN - 4/2/2021, 1:40 PM



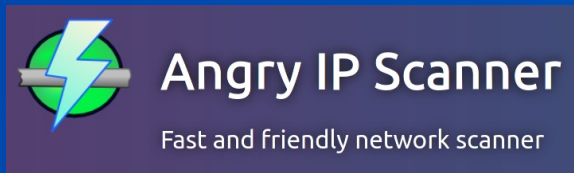
Conti affiliates use ProxyShell Exchange exploit in ransomware attacks

Written by Sean Gallagher, Peter Mackenzie

Shitrix: Hackers target unpatched Citrix systems over weekend

 Graham Cluley • [@gcluley](#)
12:14 pm, January 13, 2020

Look for the slightly inordinary



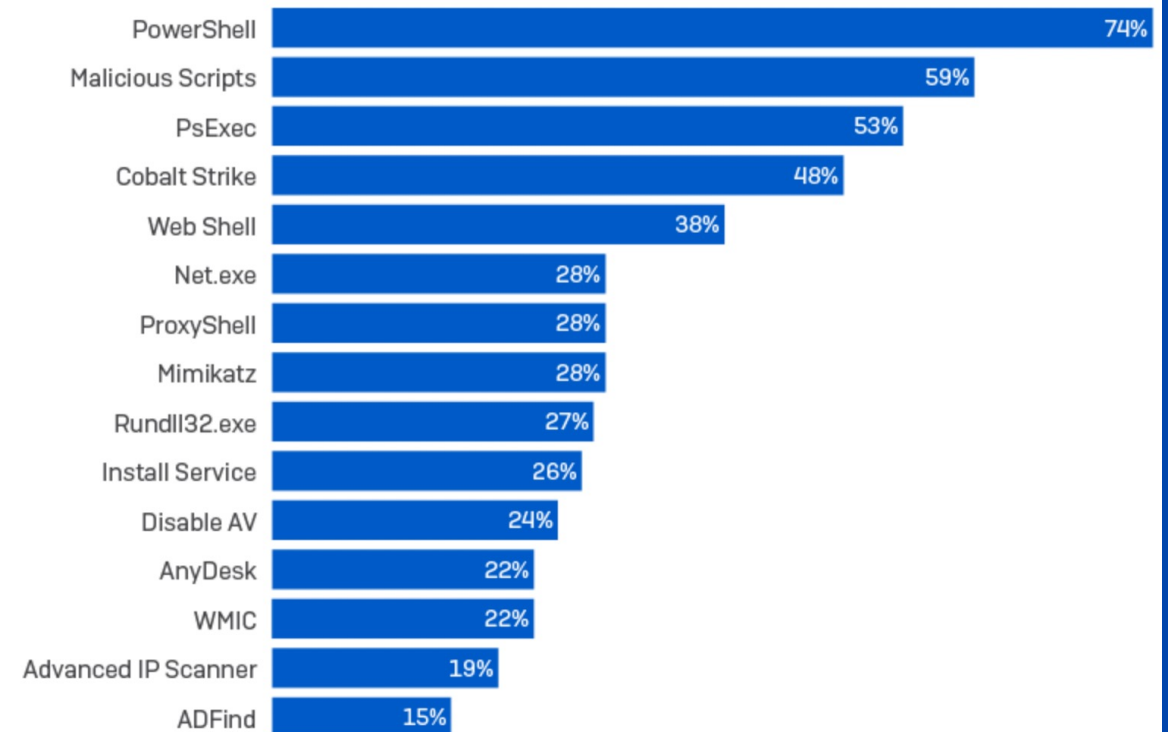
```
mimikatz

mimikatz is a tool I've made to learn C and make some experiments with Windows security.
It's now well known to extract plaintext passwords, hash, PIN code and kerberos tickets from memory. mimikatz can
also perform pass-the-hash, pass-the-ticket or build Golden tickets.

..... mimikatz 2.0 alpha (x86) release "kiki zn C" (Apr  8 2014 22:02:03)
.._.._.._
.._ / \ .._ /* * *
.._ \ / .._ ( Benjamin DELPY "gentilkiwi" ( benjamin@gentilkiwi.com )
.._ = .._ https://blog.gentilkiwi.com/mimikatz (os,oo)
"....." with 13 modules * * */
```



Top Artifacts Used in Attacks 2021



Combos and oddities



Change Management Process

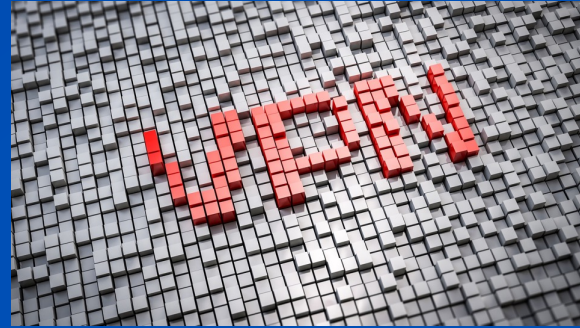


Layers!



- Not just defense in-depth, paints a picture
- Context
- A trigger to begin an investigation
- Early detection, early eviction
- Forensics

Authentication

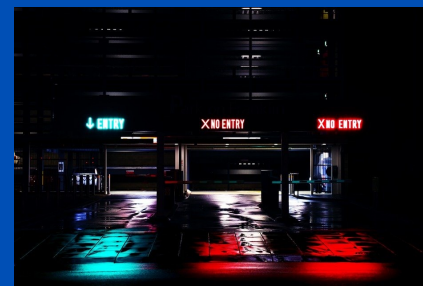


+

- Password managers
- MFA
 - TOTP
 - Push
 - Tokens
- Cookies



=



Threat Hunting



SOPHOS