

October 2020

How did the Pandemic change Cybersecurity?

And what do we do about it?

PRESENTED BY:

Raymond Pompon, Director F5 Labs



Hi nice to meet you,
I'm **Ray**.

A little bit about me...

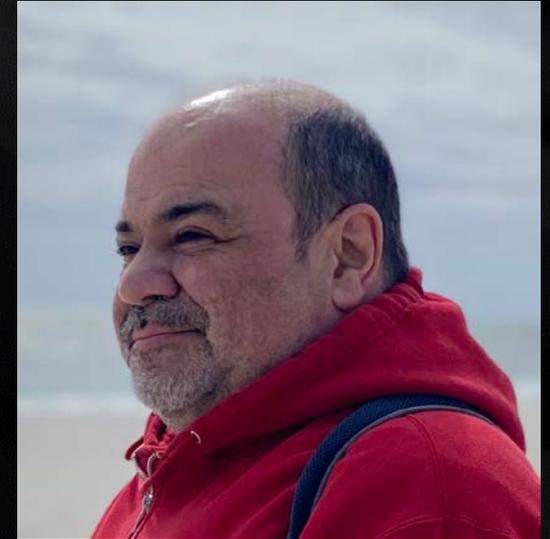
Raymond Pompon
Director, F5 Labs

20+ years in InfoSec—CISSP

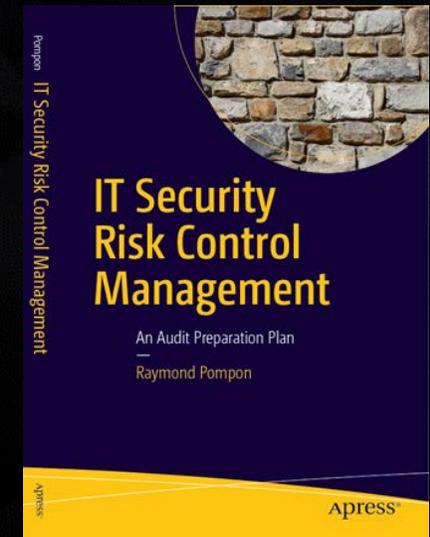
Board Member of Delaware
chapters of InfraGard, ISC²

30 years in IT

Author and Speaker



r.pompon@F5.com
@dunsany





Questions we will try to answer

1. How did the pandemic change business and IT practices, and what are the cyber security implications for the remote worker?
2. What new cyber threats have arisen from the pandemic?
3. What new fraud schemes have emerged?
4. What can we expect to see in this “new normal”?



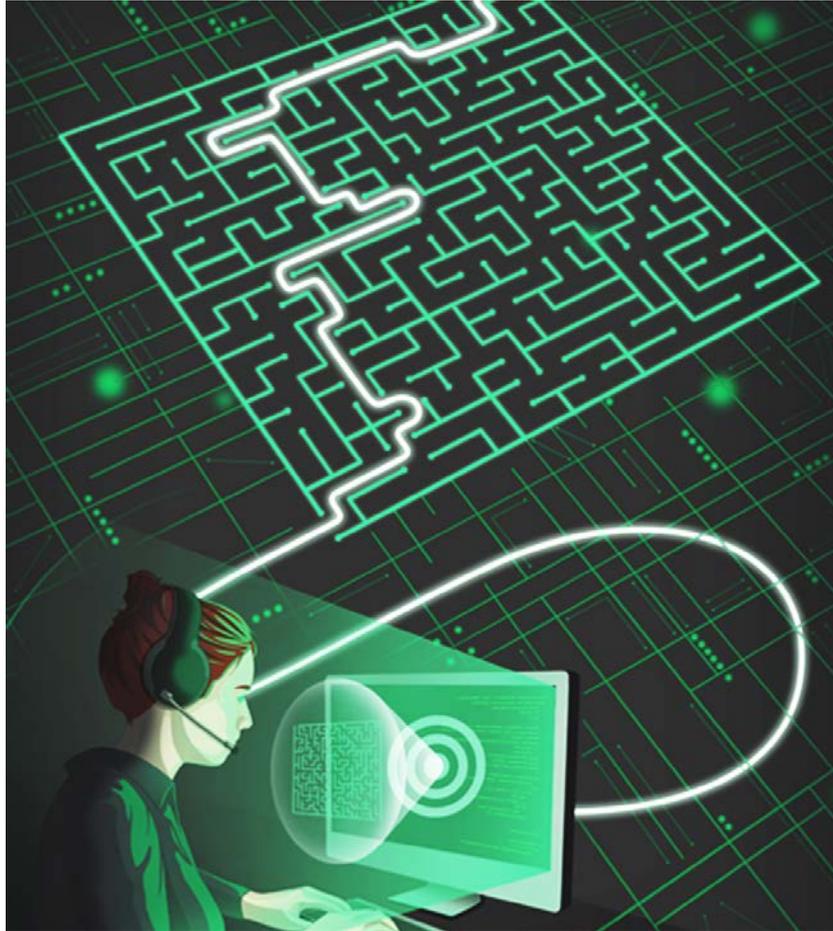
How did the pandemic **change** business and IT practices?

And what are the cyber security implications for the **remote worker**?





Business Changes Reflected in Online Traffic



SH=PE

Part of F5

- **Retail online traffic up 20%**
- **International money transfers down 14-35%**
- **Investment accounts up by 56%**
- **Travel bookings down 75%**
- **Grocery delivery up 400%**



Hypergrowth of Remote Access

Carefully planned?

Easy vs Secure?

Very visible, very attractive

The screenshot shows the Shodan search interface with the query 'port:3389'. The top navigation bar includes 'Shodan', 'Developers', 'Monitor', and 'View All...'. The search bar contains 'port:3389' and a search icon. Below the search bar are buttons for 'Exploits', 'Maps', 'Images', 'Like 104', 'Download Results', and 'Create Report'. The main content area displays 'TOTAL RESULTS: 4,821,408'. Below this is a world map showing the distribution of results by country. To the right of the map is a table of 'TOP COUNTRIES'. Below the map and table are sections for 'TOP ORGANIZATIONS' and 'TOP OPERATING SYSTEMS'. On the right side of the screenshot, there is a 'New Service' notification and two search results for IP addresses: '34.96.116.123' (Google Cloud) and '136.34.31.138' (Google Fiber). Both results show they were added on 2020-09-18 and are located in the United States, Kansas City. There are also tags for 'cloud' and 'self-signed'.

Shodan Developers Monitor View All...

SHODAN port:3389

Explore Downloads Reports Pricing

Exploits Maps Images Like 104 Download Results Create Report

TOTAL RESULTS

4,821,408

TOP COUNTRIES

Country	Count
United States	1,565,284
China	1,281,718
Germany	183,885
Netherlands	124,385
United Kingdom	119,601

TOP ORGANIZATIONS

Organization	Count
Tencent cloud computing	657,616
Amazon.com	407,107
Microsoft Azure	396,142
Google Cloud	393,640
China Telecom	238,225

TOP OPERATING SYSTEMS

Operating System	Count
Windows 10 or Server 12	564
Windows 10	207
Windows Server 2008	134
Windows Server 2003	20
Linux 3.x	9

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

RELATED TAGS: rdp

34.96.116.123
123.116.96.34.bc.googleusercontent.com
Google Cloud
Added on 2020-09-18 18:28:25 GMT
United States, Kansas City

cloud

136.34.31.138
Google Fiber
Added on 2020-09-18 18:27:49 GMT
United States, Kansas City

self-signed

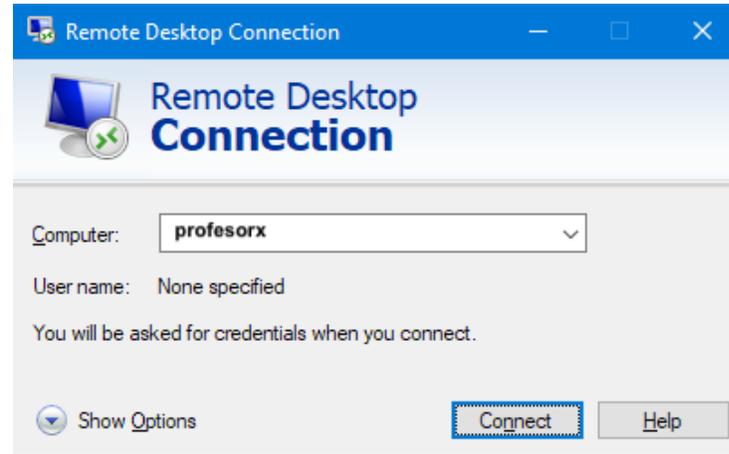




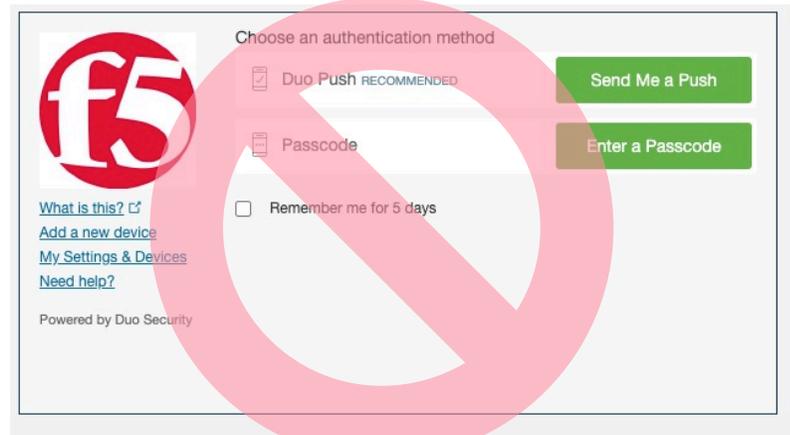
Architecture Changes Driven by Shelter-in-place



Attack surface grew



Defenses unlocked





Architecture Changes Driven by Shelter-in-place



Attack surface grew

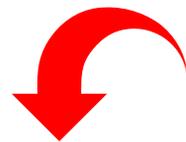


VPN (IKE & PPTP) visibility up 33%

Remote Desktop Protocol (RDP) visibility up 41%



Defenses unlocked

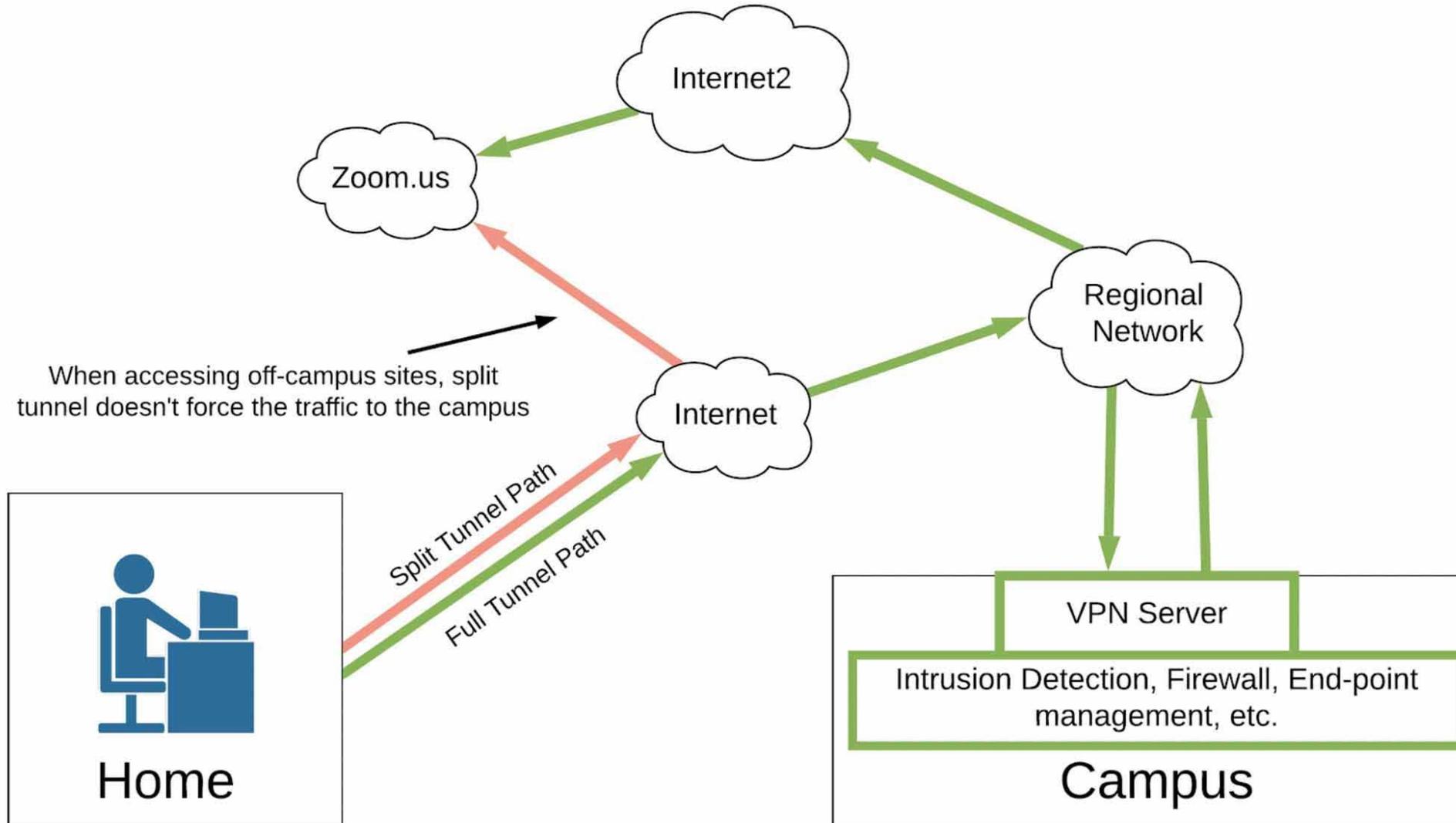


Two-factor usage reduced

VPN Split Tunneling (less filtering)

Quick explanation

Split Tunnel vs. Full Tunnel

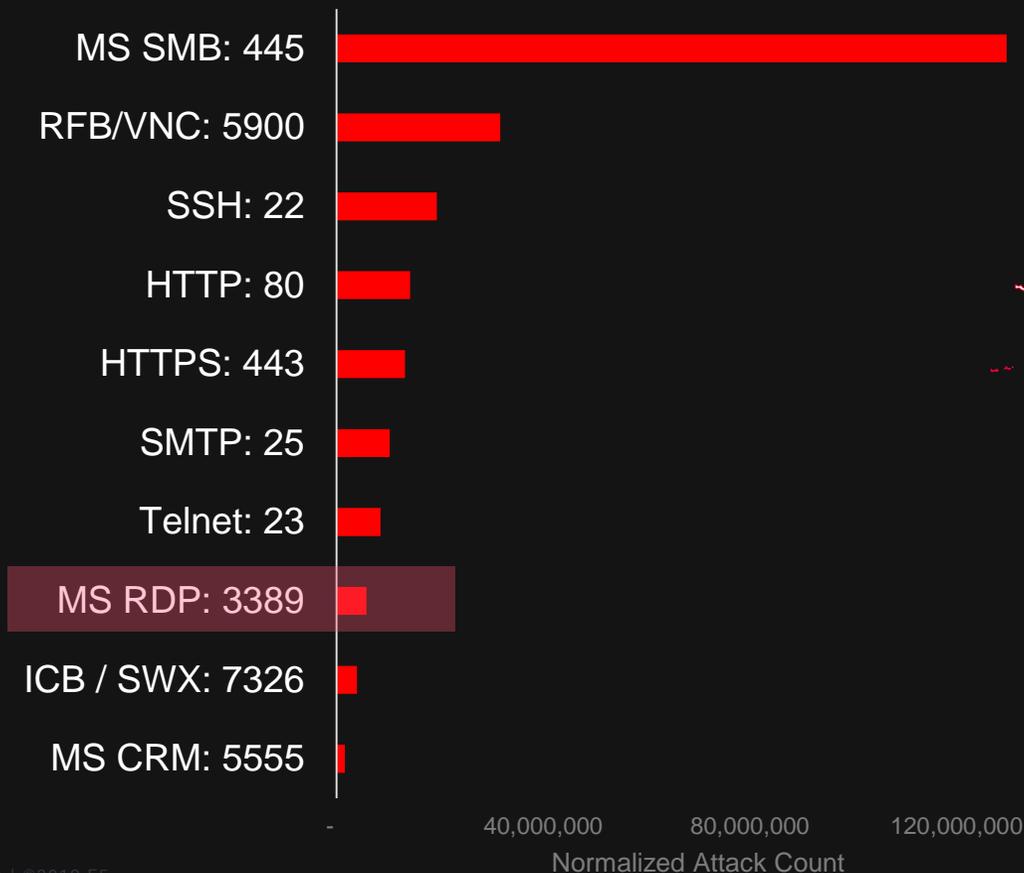




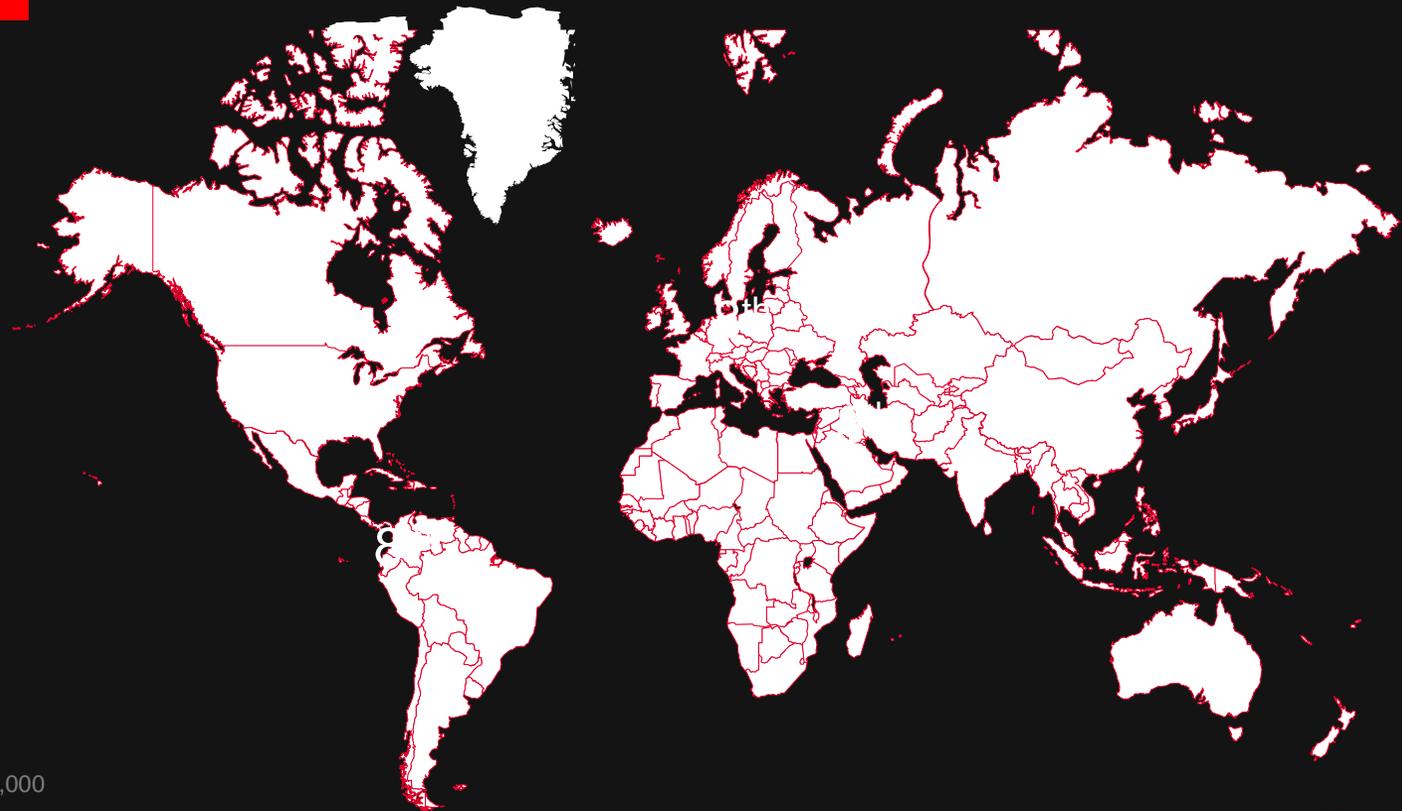
RDP is a Top Target Globally

(Pre-pandemic Q4 2019)

Global Top Targeted Ports



Top 10 position of RDP port targeting across global regions





Credential Stuffing

1 Trillion

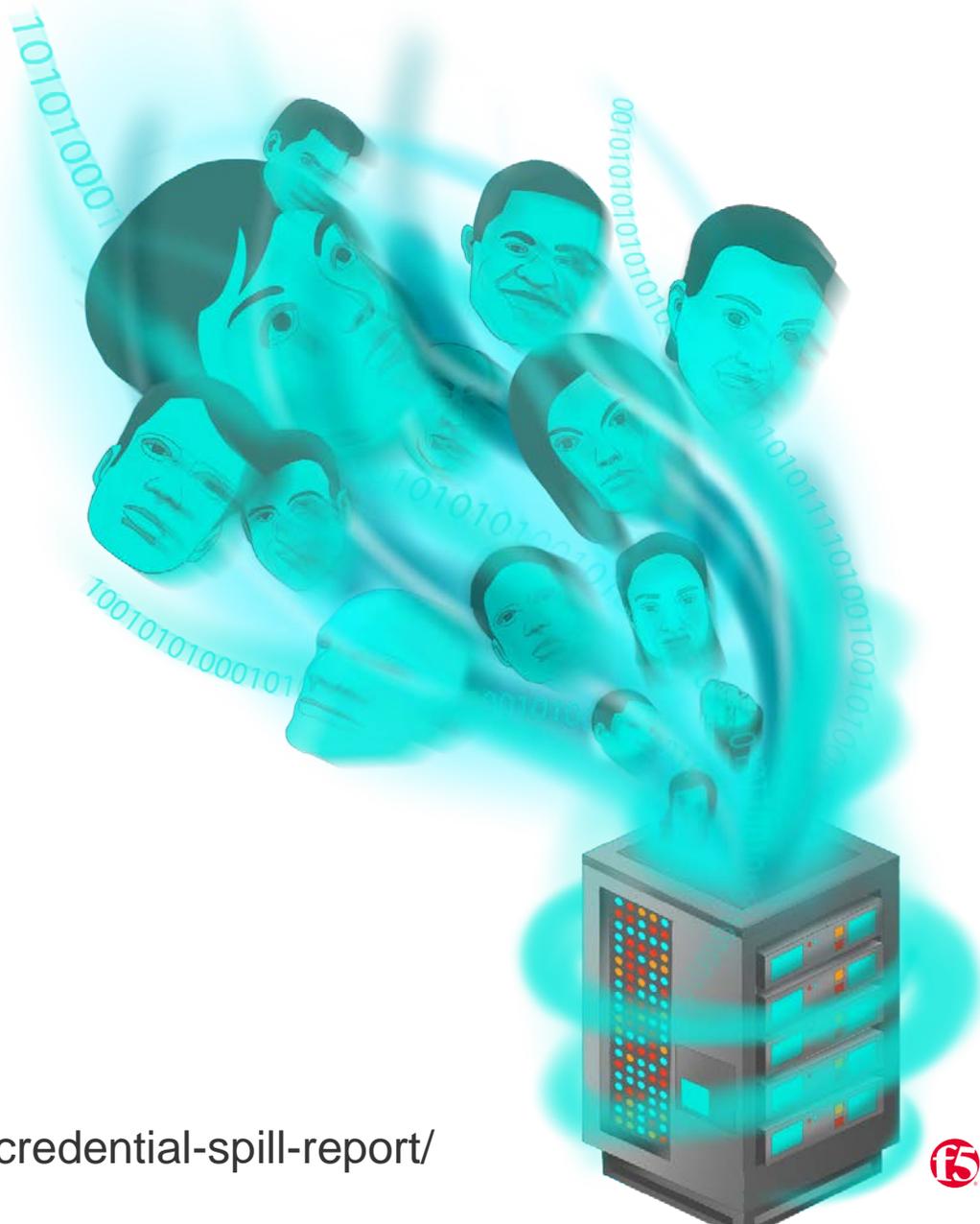
Username and passwords avail

3%

Credential stuffing success rate

3 Billion

Credentials stolen a year



In the news...

Millions of Brute-Force Attacks Hit Remote Desktop Accounts



Automated attacks on Remote Desktop Protocol accounts are aimed at taking over corporate desktops and infiltrating networks.

Brute-forcing attempts aimed at users of Microsoft's proprietary Remote Desktop (RDP) has come to light, striking millions per week. The attacks are a likely offshoot of criminals looking to take advantage of the unprecedented numbers of employees working from home amid the COVID-19 pandemic, researchers noted.

It is often used by both telecommuters as well as by tech support personnel trying to connect to an image of an employee's desktop as though the person were at their desk. A successful attack would give cybercriminals remote access to the computer with the same permissions and access to data and folders that a

Home > Hacking > Vulnerabilities

NEWS ANALYSIS

Attacks against internet-exposed RDP servers surging during COVID-19 pandemic

Two new reports show a dramatic increase in cyber attacks that target RDP servers as more people work remotely.



By **Lucian Constantin**

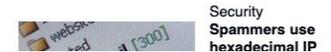
CSO Senior Writer, CSO | MAY 8, 2020 11:42 AM PDT

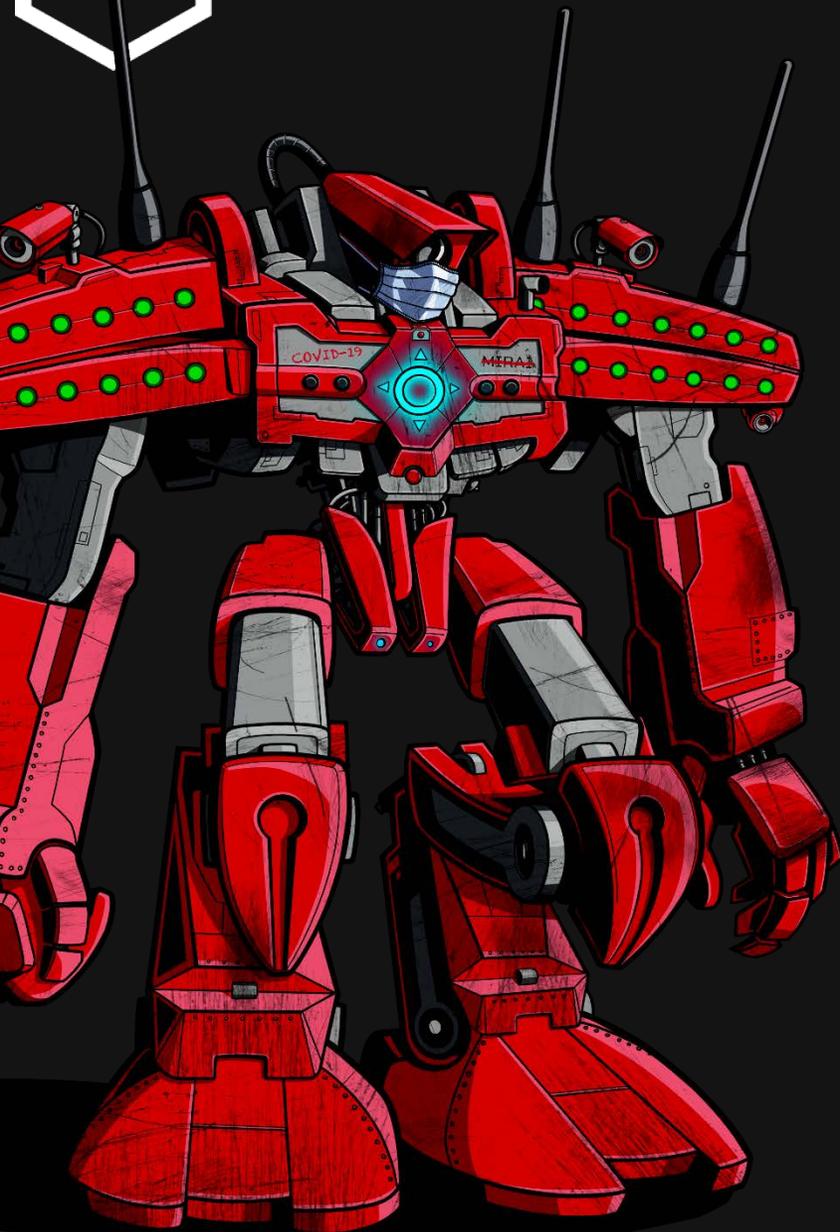
FBI says credential stuffing attacks are behind some recent bank hacks

The FBI is raising a sign of alarm about the rising number of credential stuffing attacks targeting financial institutions.

By **Catalin Cimpanu** for Zero Day | September 14, 2020 -- 18:48 GMT (11:48 PDT) | Topic: Security

MORE FROM CATALIN CIMPANU

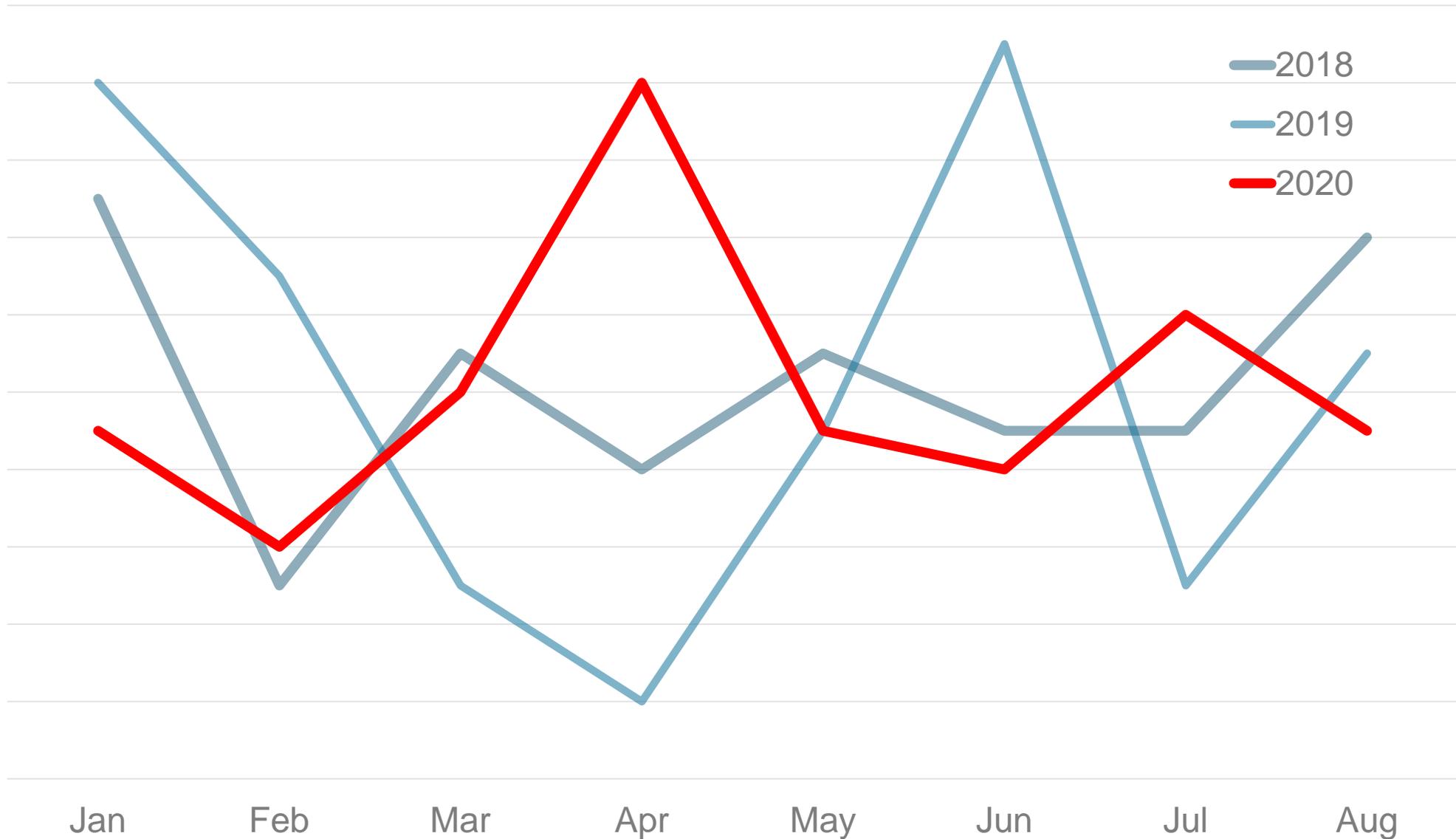




What new **cyber threats** have arisen from the pandemic?

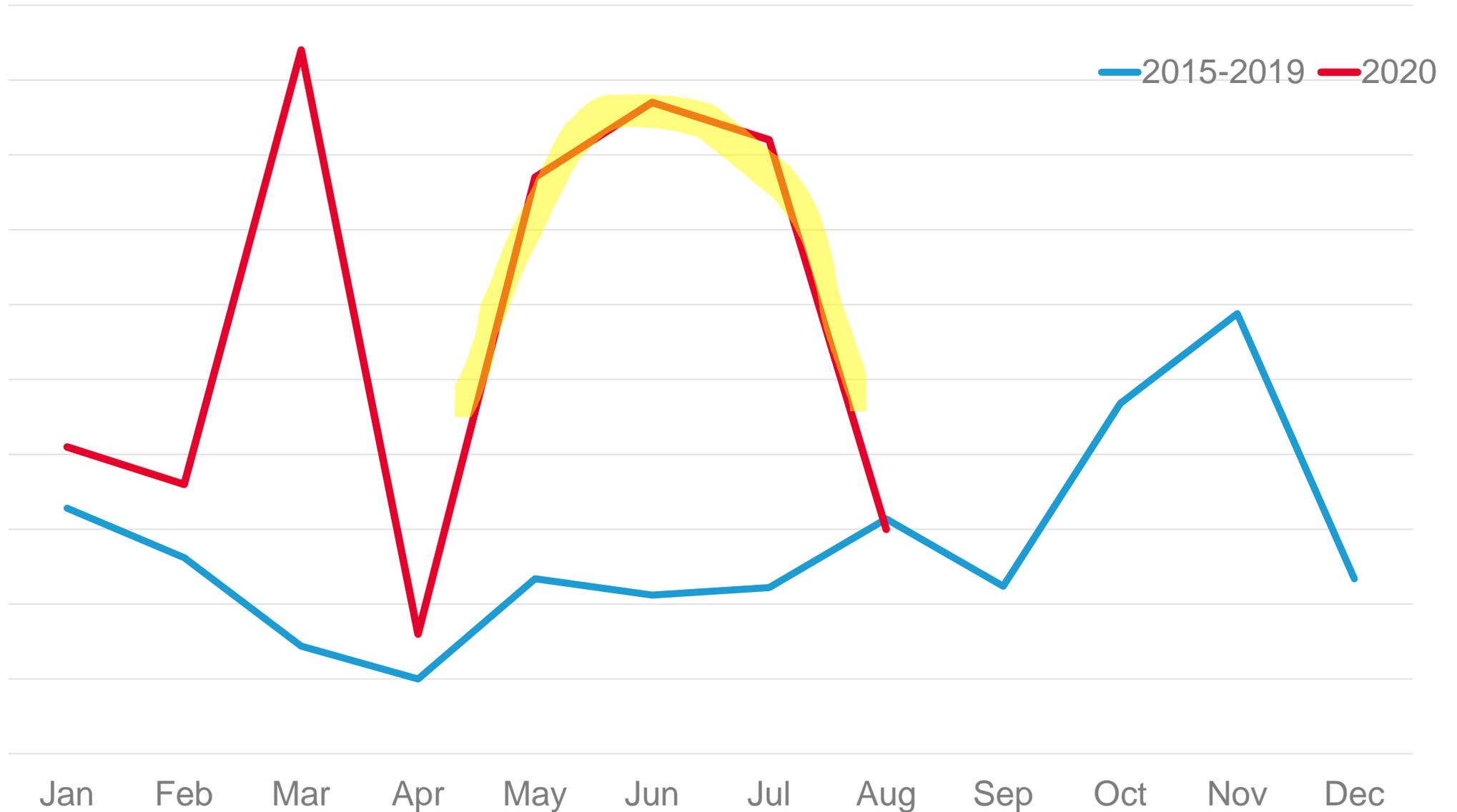


Incidents reported to the SIRT by year





F5 SOC - Phishing Attacks Rising

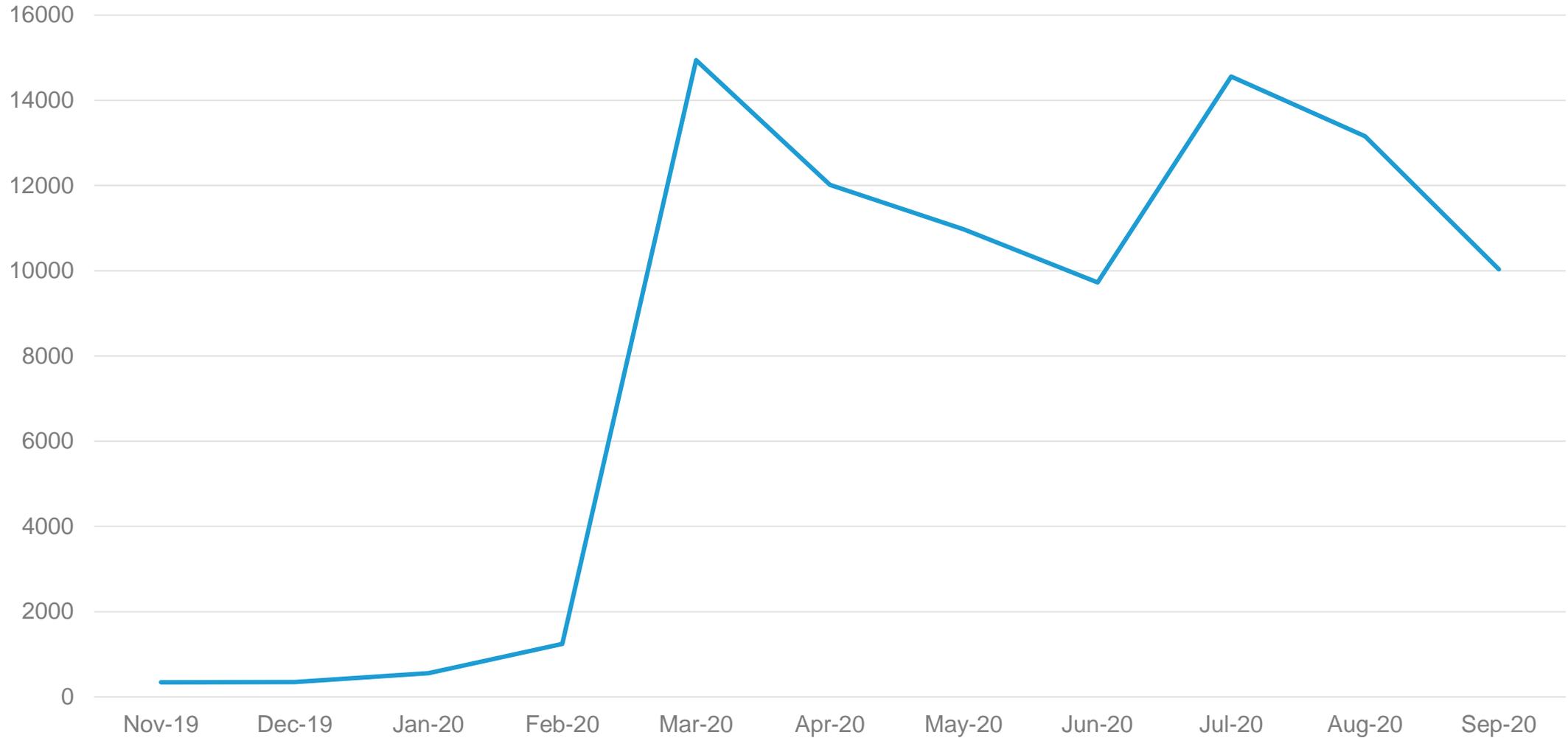


Actual Phishing Lures

- Covid-19 in your area? Please confirm your address
- Click here for COVID-19 vaccinations
- Get your COVID-19 CARES Act relief check here
- Counterfeit Respirators, sanitizers, PPE
- Fake cures for COVID-19
- Message from the World Health Organization
- Message from the Centers for Disease Control and Prevention
- Click here for Coronavirus-related information
- Donate to these charitable organizations.
- Message from Local hospital - Need patient data for COVID-19 testing
- COVID 19 Preparation Guidance
- 2019-nCoV: Coronavirus outbreak in your city (Emergency)
- HIGH-RISK: New confirmed cases in your city
- Coronavirus (2019-nCoV) Safety Measures



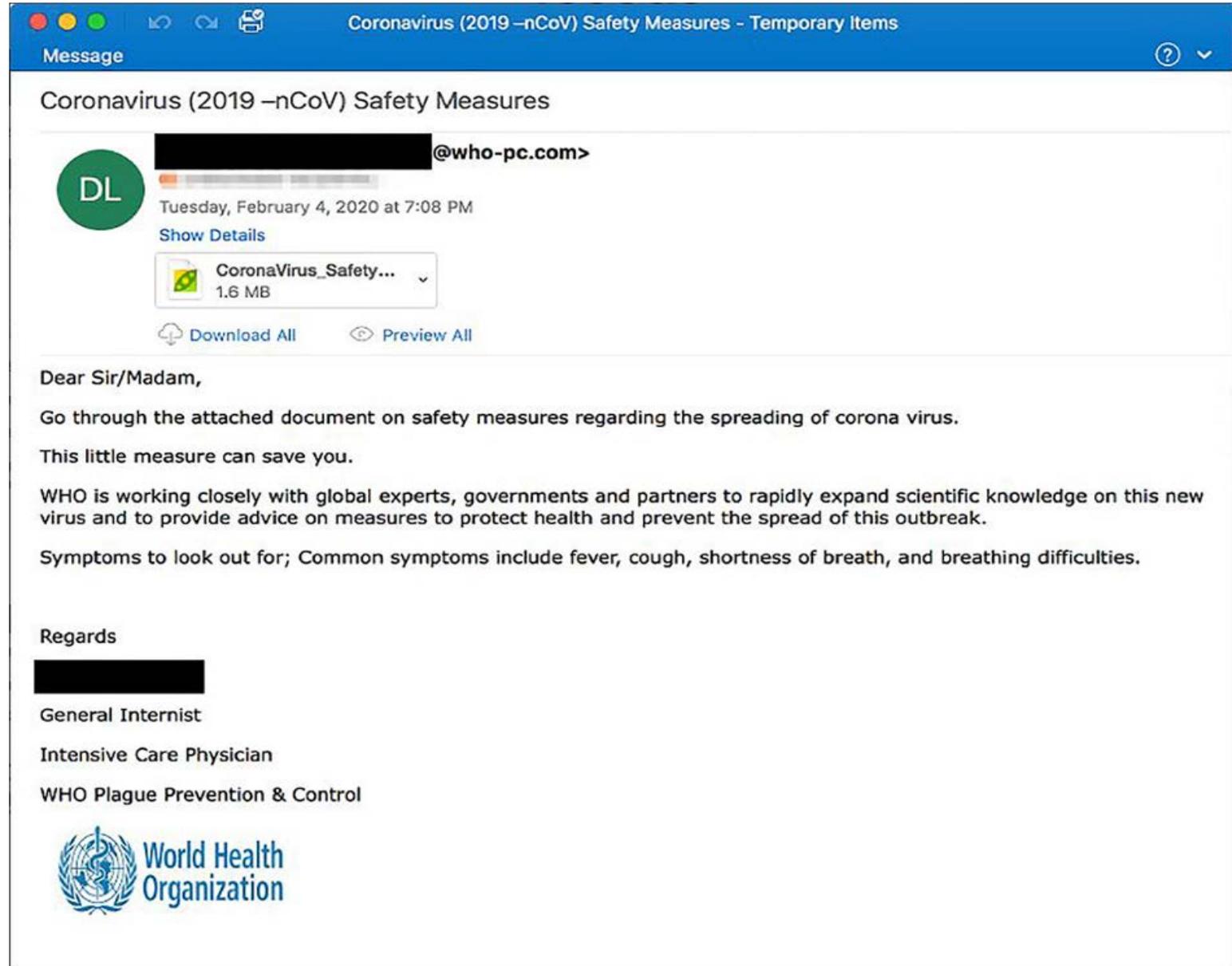
Certificates per month using the words 'covid' or 'corona'





Impersonation

- WHO
- Public Health Offices (CDC)
- Revenue Agencies
- Human Rights offices
- Charities
- Unicef
- WSJ
- FedEx





Typo Squats, Fake Domains, and a DNS Sandwich

Targetted site

<https://legitbank.com>

Hijacked site/domain

<https://blog.bichonbop.com>

<https://nab-cxthsec-reference6834576523.statrments.com>
http://dictatorads.com/hb2.financeleumi.co.il.unn_mesid2196cb8428728bd3ec6
<https://db.mutasee.com/tesbca.html>
<http://angelvengeance.com/leumi/>
<https://paypalnotic.000webhostapp.com/coil255/coil2/>
<https://cxtolike-logfacebuuk.000webhostapp.com>
<https://ib.nab.com.cx.blocked.services/login>
<https://gooddeypeople.club/amzccadvadmin>
<https://gooddeypeople.club/ebayadmin>
https://hundeteamschule-shop.de/webinar_cxth/info/
<http://ffreebies.com/new/Netfinance.html>
<http://ffreebies.com/new/Erste%20finance%20and%20Sparkassen%20Login%20-%20Passwort.html>
<https://financeing-nab.com.cx>
http://summiturgentcare365.com/Service/login/www.winfinance.gr/sites/idiwtes/el/Pages/financeing.winfinance.gr/_Login/EBlogin031a.html
<https://essfiresafe.com/Service/login/www.winfinance.gr/sites/idiwtes/el/Pages/>
<http://www.nabib.com.cx.oceancity.accountlogin.login.now.webdemoic.com/>
<http://nab-account.logged-system.recover-card.siliteyusiwangi.xyz>
<http://nabib.com.cx.login.oceancity.notifythecustomer.log.cxss.n4tools.com>
<https://107.174.25.130:446/config.php>
<https://139.60.163.56:446/response.php>
<http://mail.ib.nab.com.cx.x51abvenfq5abn.ib-national-con.com/def/mobile/login/>
<https://erste978887452.blogspot.com/JEELRJRLSMS>
<https://bestofhealthip.club/wp-content/gw/5df41b09aec0add76700d37ded6af2b0c/>
<http://erstefrensm9874457821.blogspot.com/>
<http://mail.benstokes.com/dir-bak/pay/il/c383a8f2eef55d511612ad103e547f>
<http://www.legendsofeightysix.com/Service/login/www.winfinance.gr/sites/idiwtes/el/Pages/defcxlt.html>
<https://jobily.co.uk/data/userData/secure/lb/login.php>
<http://moonsuntravel.com/nab/>
<https://ubagroup-private.com/>
<https://nationalcxstralianfinance.herokuapp.com/login/>
<http://www.nabacts.com/>
<http://www.nab.ib.nabib.login.oceancity.userandpassword.required.ormecorp.com/>
<http://gopay.com.my/hr/Erste%20Netfinanceing.html>
<http://qesota-71.gq/hr/Erste%20Netfinanceing.html>
<https://sign.supportservice-login.sukakamusell.com/nab.com.cx>
<https://ib.nab.com.cx.nz-01110data.tk/customer-help/center/profile-check/index.html>
http://pirometer.ru/_cxtogenerated/components/bcExternalTinyMce/tinyMce/plugins/index.php
<https://bit.ly/37n3UeL>
<http://zen-do.net:32000/freebusy/inc/il/index.php>
<http://akdenizmefrusat.com/32000/freebusy/inc/il/index.php>
<https://nab.com.cx.financeing-security.services/def/mobile/>
<http://nab.inform.jrelectricalservices.com.cx>
<http://nab.support-info.marketingmob.com.cx>
<http://serv-nn.rv/engine/spaw2/uploads/files/dremn.phhh5p>
<https://namunitregistry.com.cx/ofs>
<https://www.cashpassport.com.cx/nab/dashboard/>

Fake site example 1

<https://legitbonk.com/>

Fake site example 2

<https://blog.bichonbop.com/.tmp/legitbank-online-banking-login/>

Fake site example 3

<https://excitingoffer.legitbank.com.bichonbop.com>





Malware rides in on the phish



F5 Labs @F5Labs · Apr 27

#Mirai calls itself #COVID and wants to get into your home, despite order to "hunker down" and it's not the only malware joining that party. Write up and details of this variant's target's on F5 Labs: go.f5.net/59aye



Malware Multiplying



Inject into login sequence for:

- Retail eCommerce
- Shipping
- Banks
- Entertainment
- Food Delivery
- Online Auction

<https://www.f5.com/labs/articles/threat-intelligence/qbot-banking-trojan-still-up-to-its-old-tricks>

Malware Web Inject



Security Information

Unfortunately, due to unforeseen technical work in the online system we are having trouble identifying you. You'll have to prove your identity by following the instructions below. This check is one-time, and in the future you will be able to use your account without problems. Our team apologizes for any inconvenience

CREDIT OR DEBIT CARDS

- * Name on card
- * Card number
- * Expiration date
- * CW

CONTINUE

What new **fraud** schemes have emerged?





Scattered Canary

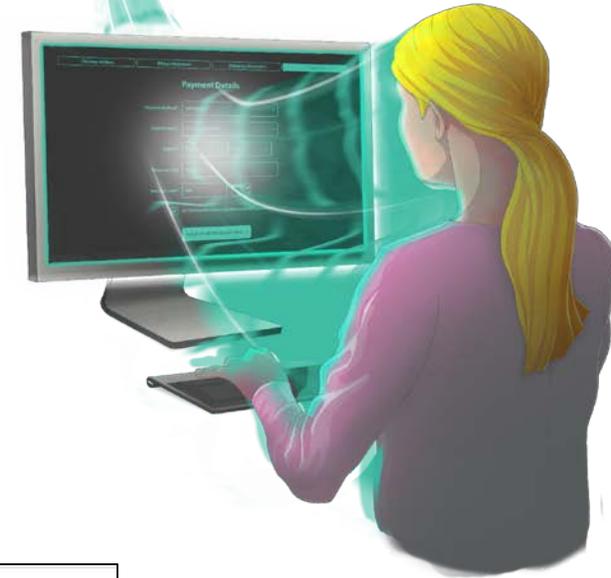
Washington halts unemployment payments for 2 days after finding \$1.6 million in fraudulent claims amid coronavirus pandemic

May 14, 2020 at 2:03 pm | Updated May 14, 2020 at 7:06 pm



'Hundreds of millions of dollars' lost in Washington to unemployment fraud amid coronavirus joblessness surge

May 21, 2020 at 6:55 am | Updated May 21, 2020 at 11:13 pm



Menu **The Seattle Times** **Times Watchdog** Log In | Subscribe | Search

CORONAVIRUS LOCAL BIZ SPORTS ENTERTAINMENT LIFE HOMES OPINION | JOBS AUTOS EXPLORE All Sections

Traffic Lab Project Homeless Crime Local Politics Education Eastside Watchdog News Obituaries FYI Guy Westneat Ishisaka

Business | Crime | Economy | Local News | Nation & World | Times Watchdog

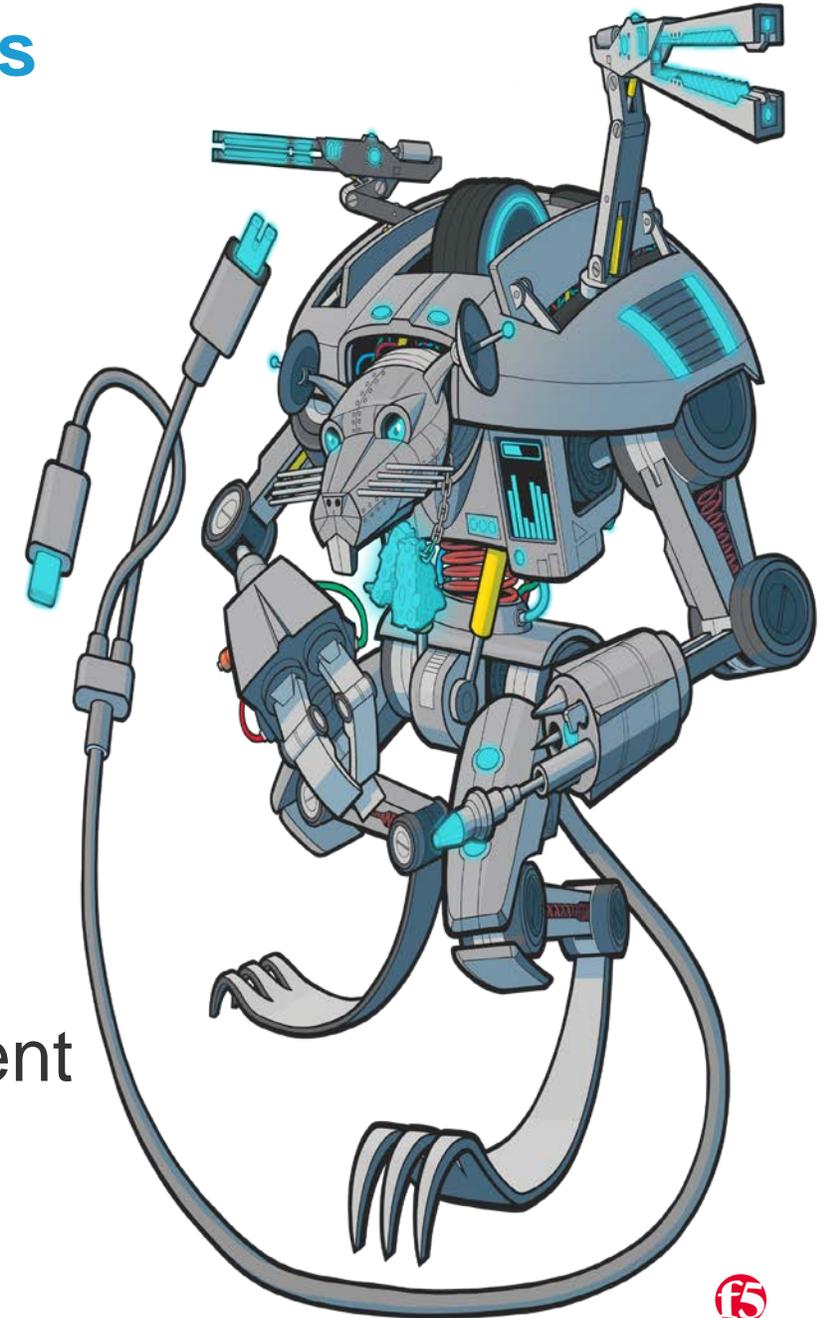
How missed 'red flags' helped Nigerian fraud ring 'Scattered Canary' bilk Washington's unemployment system amid coronavirus chaos

May 24, 2020 at 6:00 am | Updated June 4, 2020 at 6:18 pm

By [Jim Brunner](#), [Paul Roberts](#) and [Patrick Malone](#)
Seattle Times staff reporters

Bots attack e-tailers, restaurants

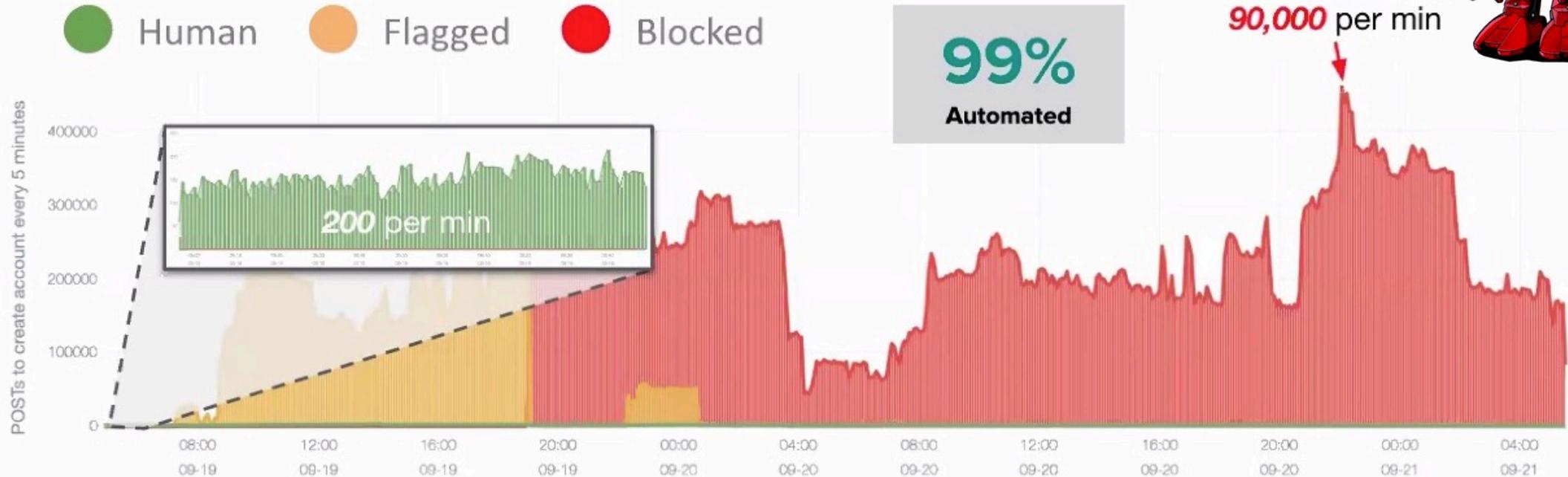
- Create synthetic identities
- Use stolen identities/credentials
- Fraudsters pose as discount providers on social media to place real orders with stolen credit cards
- High unemployment -> Money mule recruitment



Fraud via automation

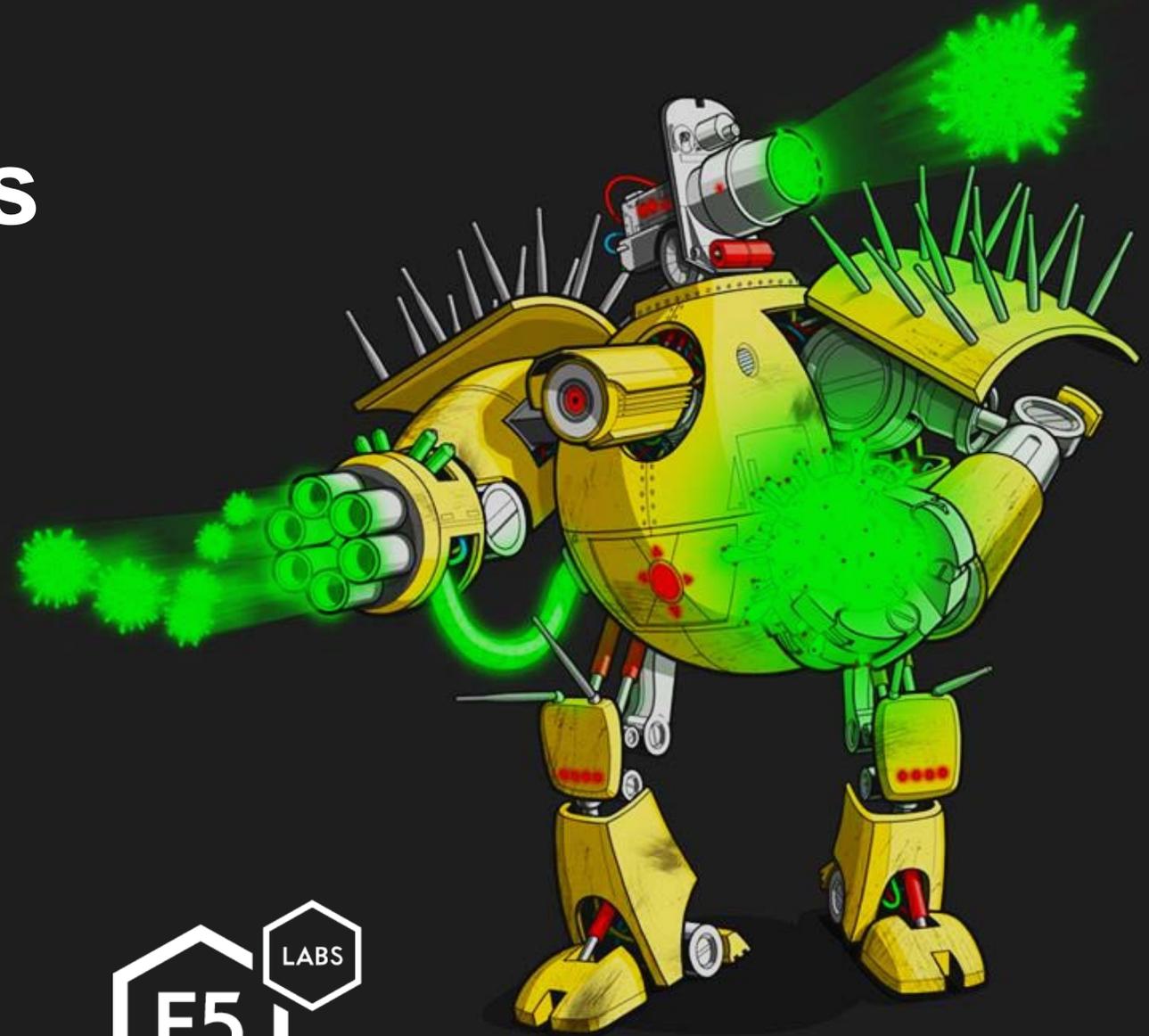
Create account attack against large international retailer

Attack intended to exploit refer-a-friend loyalty program



122 million attempts to create **59 million** accounts

What can we expect to see in cyberthreats this “**new normal**”?





Phishing evolves

Pre-pandemic lures

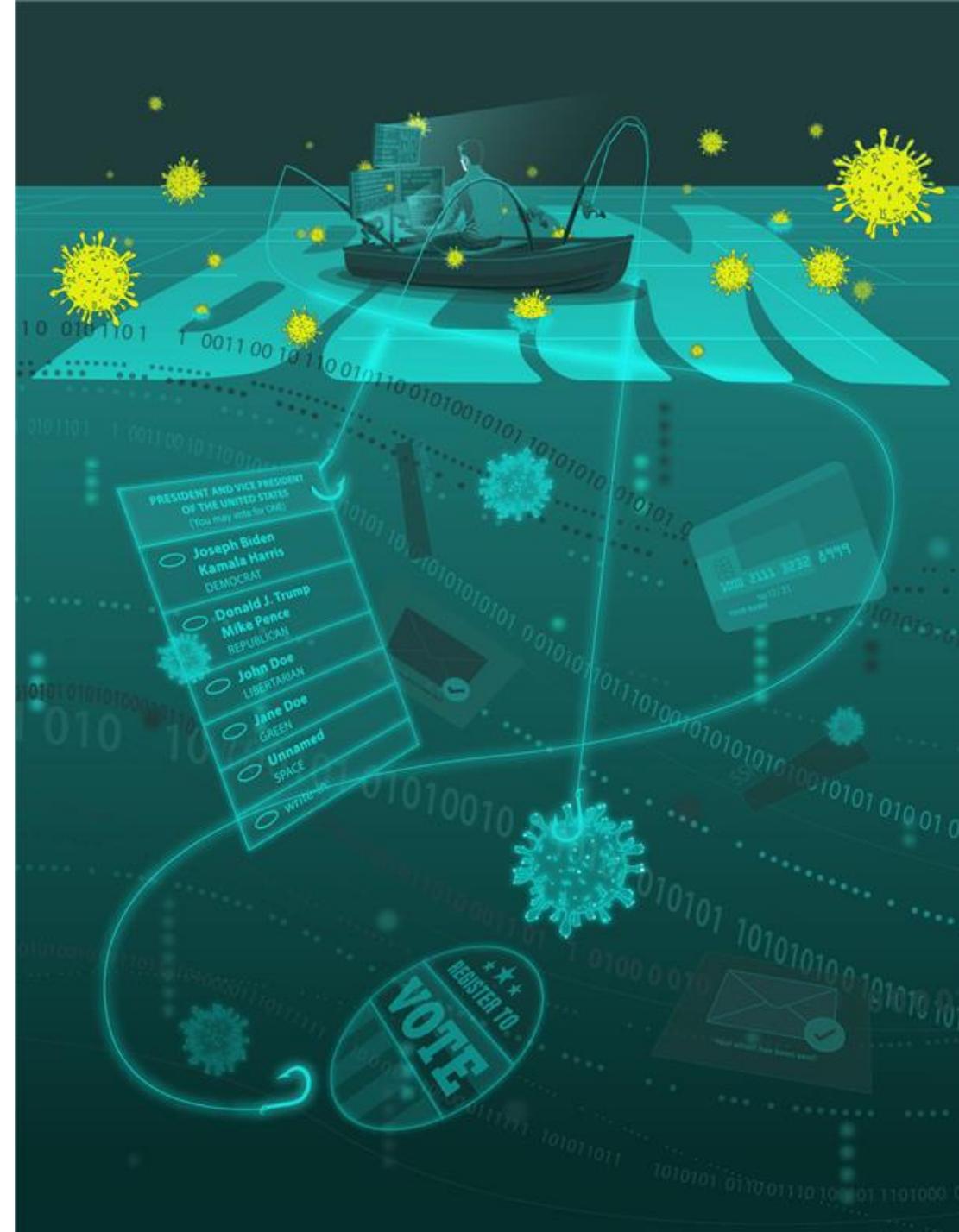
- Websites - bank notices, fake confirmations/alerts
- Attachments - Invoices, shipping information, resumes

Pandemic lures

- COVID-19 update, Hospital notify, Cures, N95/PPE, Donations

New Normal lures

- BLM, Pandemic Stimulus, Elections



Ransomware is Big Business



SALE!

CUSTOM-MADE RANSOMWARE
~~\$470.00~~ **\$350.00**

Ransomware is a form of malware where person attack victim system with malicious code. Their intent is to lock out of system and encrypt important and sensitive data

1 **Add to cart**

Category: [Hacking Services](#) Tag: [CUSTOM-MADE RANSOMWARE](#)
[Report Abuse](#)

LUMOS Hacking Group Custom Ransomware

DESCRIPTION SHIPPING REVIEWS (0) VENDOR INFO MORE PRODUCTS

Description

CUSTOM-MADE RANSOMWARE

Do you remember wannacy? They earned over \$ 100,000 from ransoms. We make to computers or Android.

What is ransomware?

Ransomware is a form of malware where person attack victim system with malicious code. Their intent is to lock out of system and encrypt important and sensitive data. Further, they demand ransom from you before they provide a decryption key for your locked system and encrypted data.

Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Ransomware can be devastating to an individual or an organization.

Attack vector is usually

- Phishing delivered malware or
- Password attack on remote login
- Popular unpatched vulnerability

Ransomware attackers penetrate and wait

Common Targets:

- Health care
- Cities
- Schools
- Health services

*Ransom based
on victim size:
\$15k for small,
\$150k+ for larger*





We are the Fancy Bear and we have chosen you as target for our next DDoS attack.

Please perform a google search for "Fancy Bear" to have a look at some of our previous work.

Your whole network will be subject to a DDoS attack starting at Wednesday (in 5 days). (This is not a hoax, and to prove it right now we will start a small attack on your DNS servers. It will not be heavy attack, and will not cause you any damage, so don't worry at this moment.)

There's no counter measure to this because we will be attacking your IPs directly (AS13588) and our attacks are extremely powerful (peak over 2 Tbps)

What does this mean? This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers.

How you can stop this? We will refrain from attacking your servers for a small fee. The current fee is 20 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay attack will start, fee to stop will increase to 30 BTC and will increase by 10 Bitcoin for each day after deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: `ly3v2SauSylkhZnoXmVHqDjzaTxB4YRXv`

Once you have paid we will automatically get informed that it was your payment.

Please note that you have to make payment before the deadline or the attack WILL start!

What if you don't pay?

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

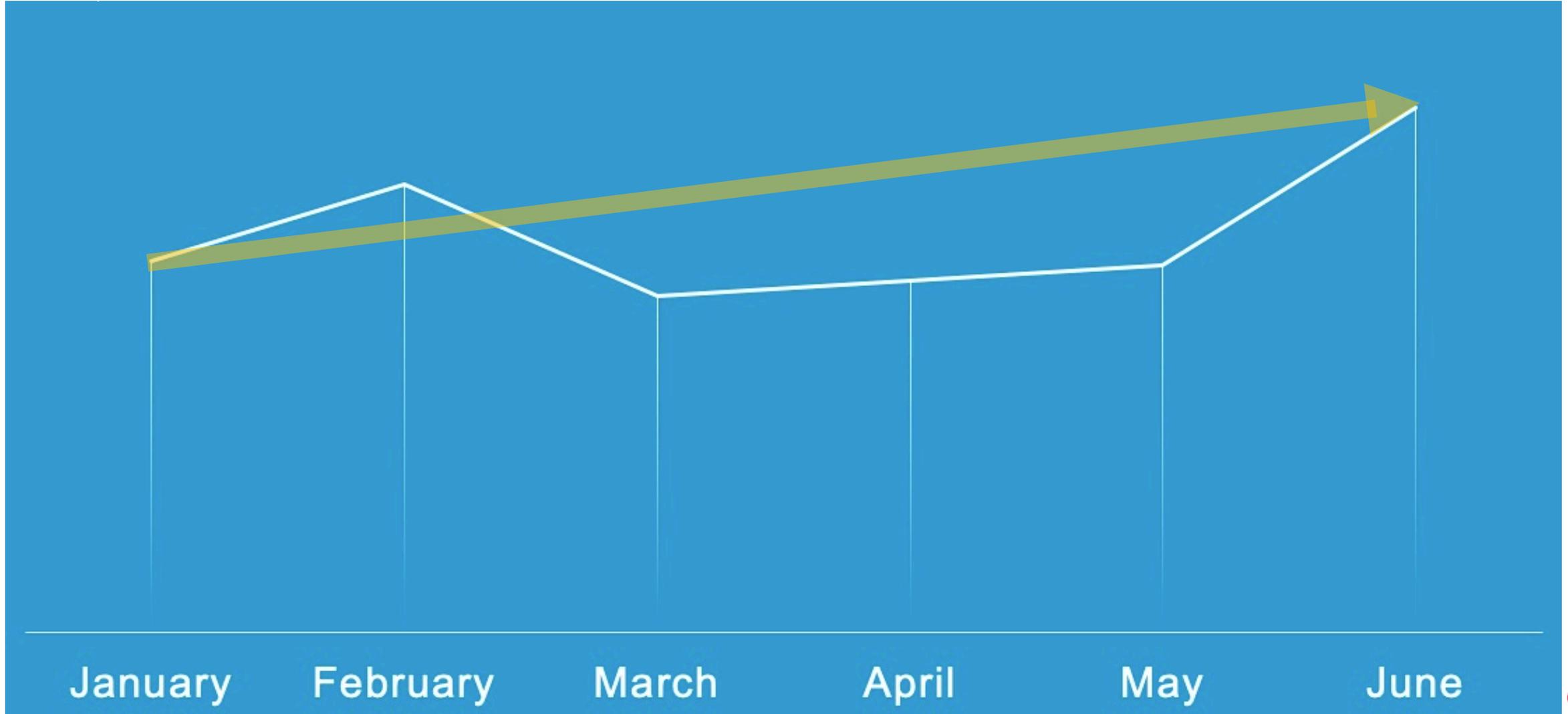
Do not reply to this email, don't try to reason or negotiate, we will not read any replies.

Once you have paid we won't start the attack and you will never hear from us again. Please note that no one will find out that you have complied.





Count of DDoS Attacks By Month Mitigated by F5 Silverline Q1 & Q2 2020





Disinfo schemes

Spreading the chaos and the hate

- Over 70 social networks infected with fake accounts
- Primary attack vector: Credential stuffing (stolen user/pass) to create fake accounts
- Create and cultivate social media accounts for months to build up a "lived in feel" and then resell



<https://github.com/podpeople/podpeople>



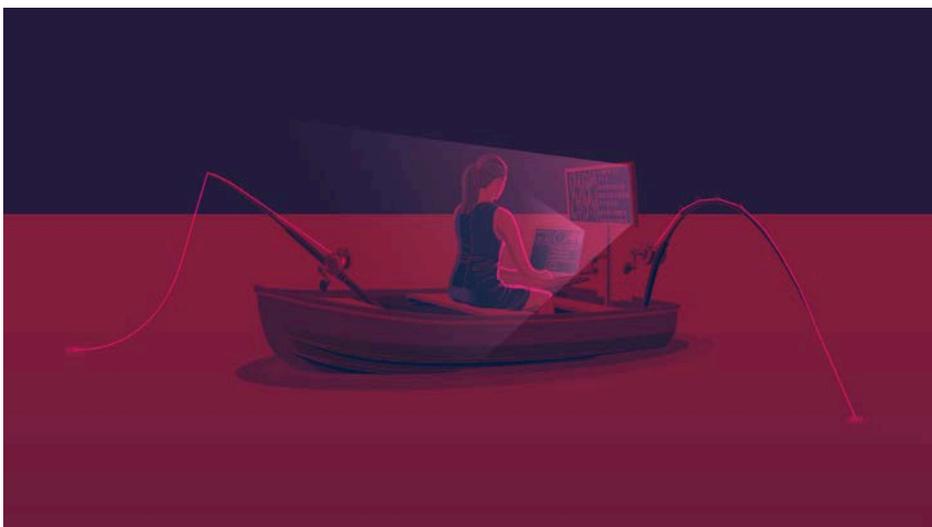
How we fight back





Watch for these Two Login Attacks

Phishing



Password Guessing via Credential Stuffing





Takeaways for Organizations

What you need to do

- Use strong authentication on any Internet-facing login (or administrative account, even on the inside)
- Patch everything you feasibly can, especially Internet-facing services
How to prioritize - <https://www.youtube.com/watch?v=w7ODzbXyCXY>
- Be wary of any email file attachments - scan them first
- Disable macros if you can
- Verify all transactions, especially when they come in via email

<https://www.f5.com/labs/articles/cisotociso/recommended-security-controls-for-2020->



Takeaways for Individuals

Personal advice

- Don't reuse passwords - different account, use a different password
- Freeze or lock your credit
- Make sure your computer, your smartphone, and your browser are patched
- Use and update anti-virus software
- Don't fall or spread misinformation – verify before you act

<https://www.f5.com/labs/articles/cisotociso/five-steps-users-can-take-to-inoculate-themselves-against-fake-news-25585>

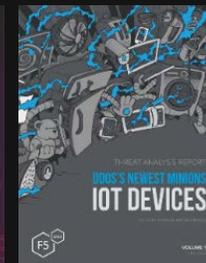
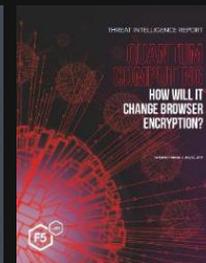
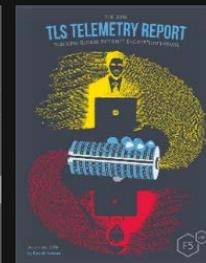
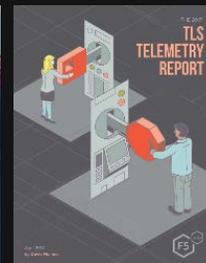
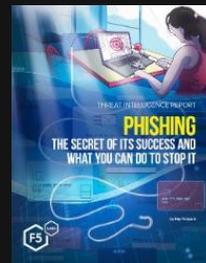
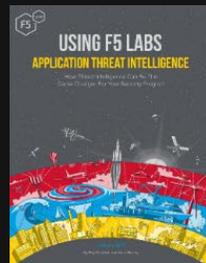
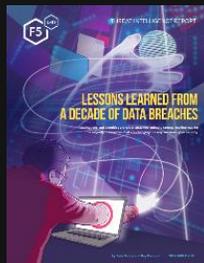
<https://www.f5.com/labs/articles/education/fraudulent-unemployment-claims-signal-consumers-to-step-up-perso>

<https://www.f5.com/labs/articles/education/how-to-guard-against-identity-theft-in-times-of-increasing-online-fraud>

F5Labs.com



General Threat Trends



F5Labs.com

Stay Up to Date by Following Us!

Tell us what you want to read about – or write for us!



Twitter



LinkedIn



Email
Updates
(1 / week)



RSS