Resolve and Evolve: Global Cyber Threats of 2021

Andrew Murphy
Director of Product Marketing , Zix

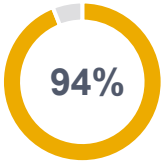
SCANTRON. SMART STARTS HERE

ZIX

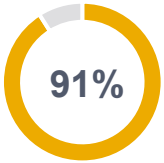
2021 Evolving Themes

- Increasing levels of Sophistication, Customization and Personalization
- Finding more Legitimate services to abuse
- Capitalizing on global trends
- Evolving to fill the void left behind by operational disruptions

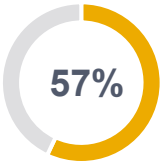
Why are we still discussing email security?



Malware delivered by email



Cyberattacks that being with a spear phishing email



Spam, Phishing, or Malware

2020 Crime Types Continued (by victim loss)

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,866,642,107	Overpayment	$51,039,922
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

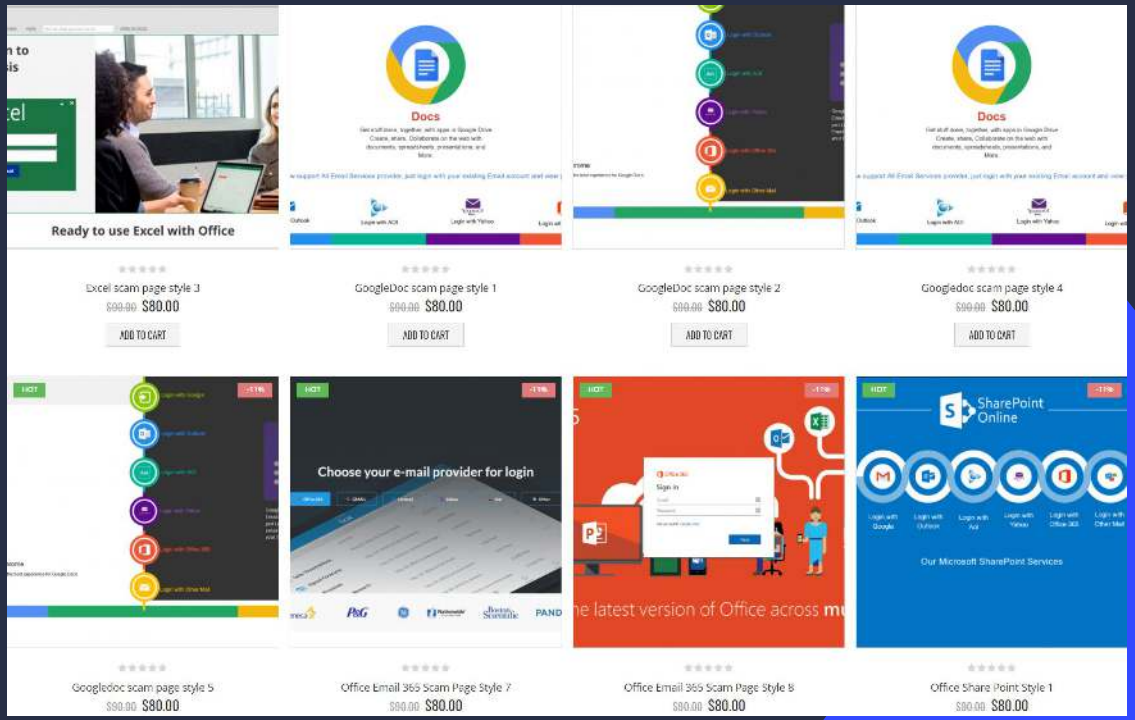
Cybersecurity Thrust into Headlines

zix

Ransomware-as-a-Service

Phishing Kits

zix



Excel scam page style 3
~~$90.00~~ $80.00
ADD TO CART

GoogleDoc scam page style 1
~~$90.00~~ $80.00
ADD TO CART

GoogleDoc scam page style 2
~~$90.00~~ $80.00
ADD TO CART

Googledoc scam page style 4
~~$90.00~~ $80.00
ADD TO CART

Googledoc scam page style 5
~~$90.00~~ $80.00

Office Email 365 Scam Page Style 7
~~$90.00~~ $80.00

Office Email 365 Scam Page Style 8
~~$90.00~~ $80.00

Office Share Point Style 1
~~$90.00~~ $80.00

Emotet Takedown… aka Operation Ladybird

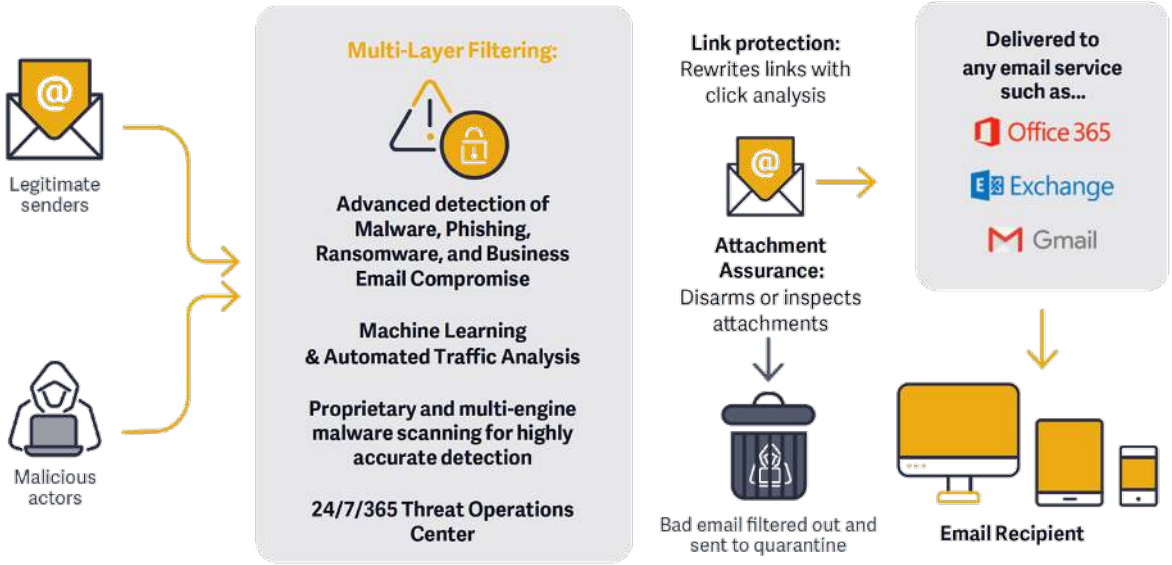
zix

Orchestrated
By Europol

Quarantined over 1
million infected systems

Disrupted future
operations

Email Threat Protection



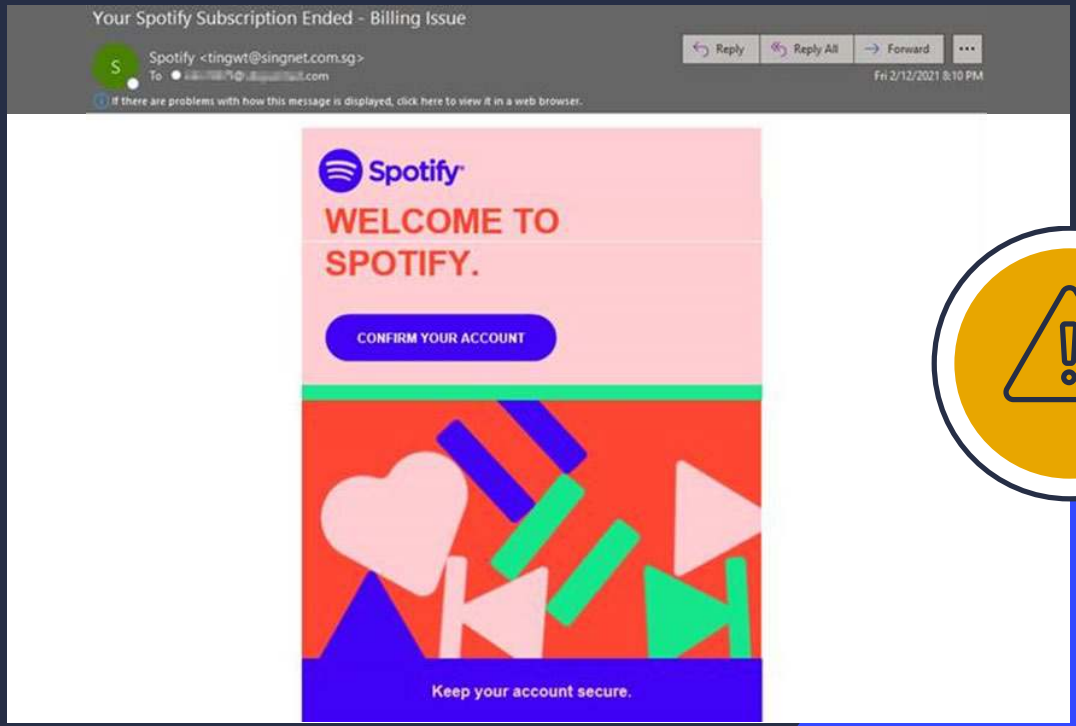
Threat Protection

- Stop spam, phishing, zero-hour malware, and business email compromise without user intervention
- Dynamic time-of-click defense and attachment sandboxing
- 24/7/365 security technicians proactively adjust defenses
- Flexible routing, email policies, and on-demand message retraction expedites enforcement
- Daily configuration checks for optimized routing and protection

Email Attack Examples

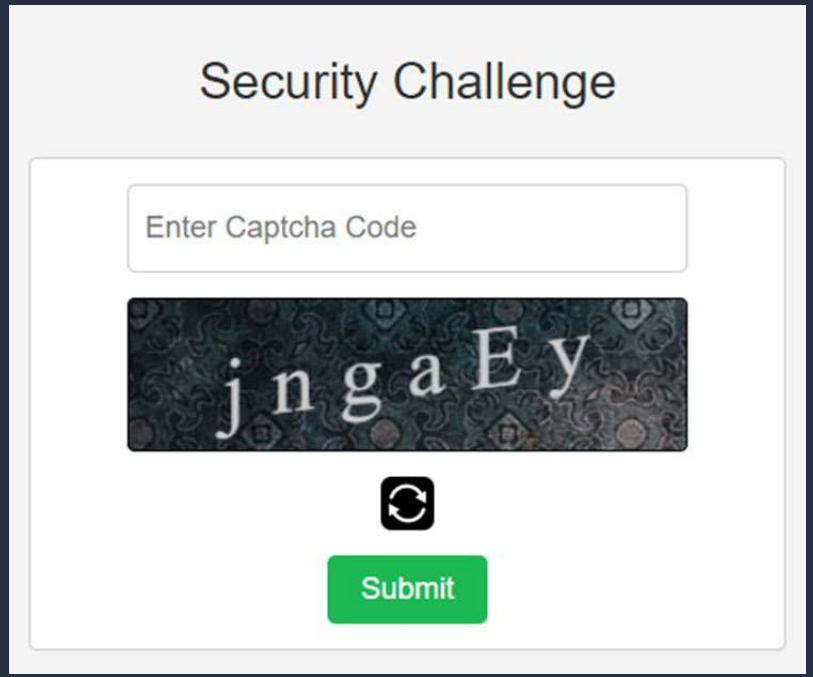
More Obfuscation – Captcha Phishing

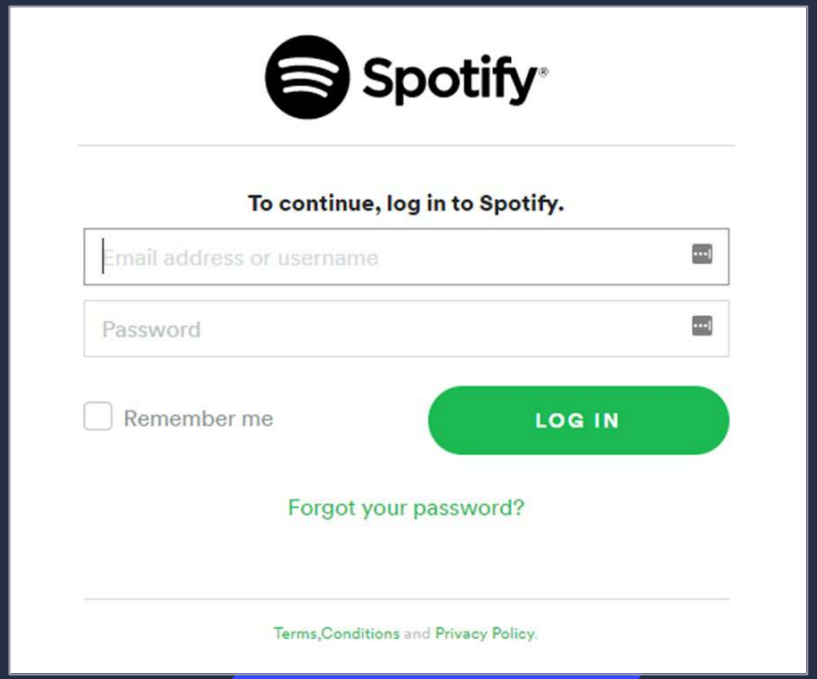
zix



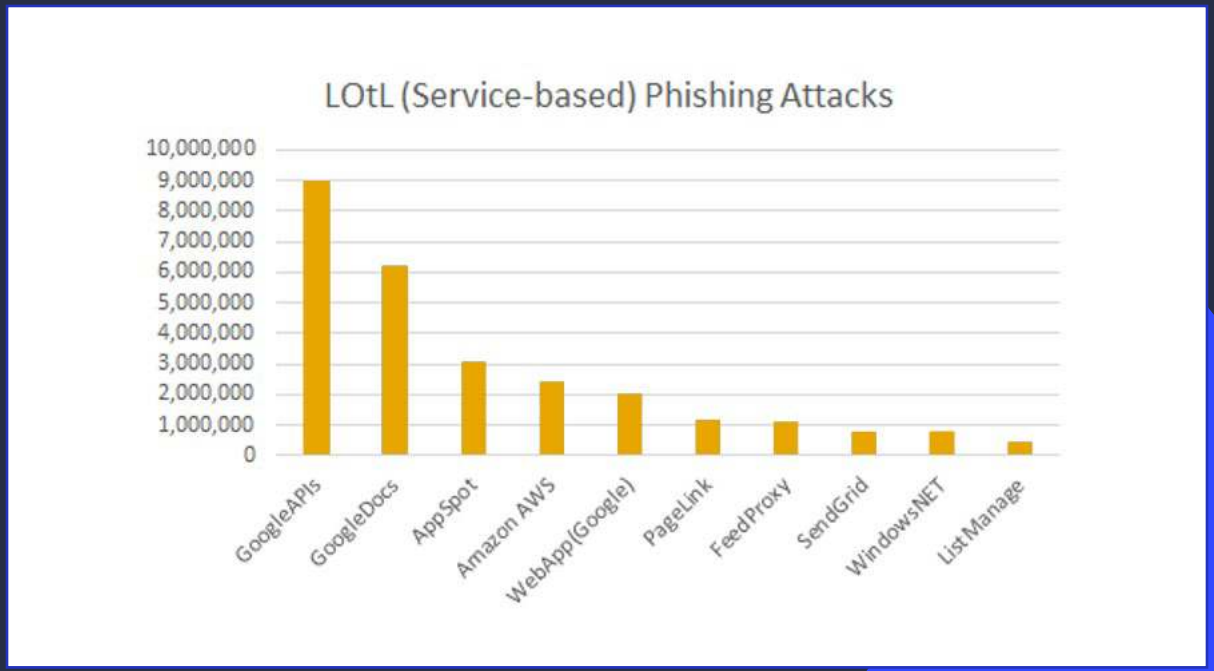
More Obfuscation – Captcha Phishing

zix

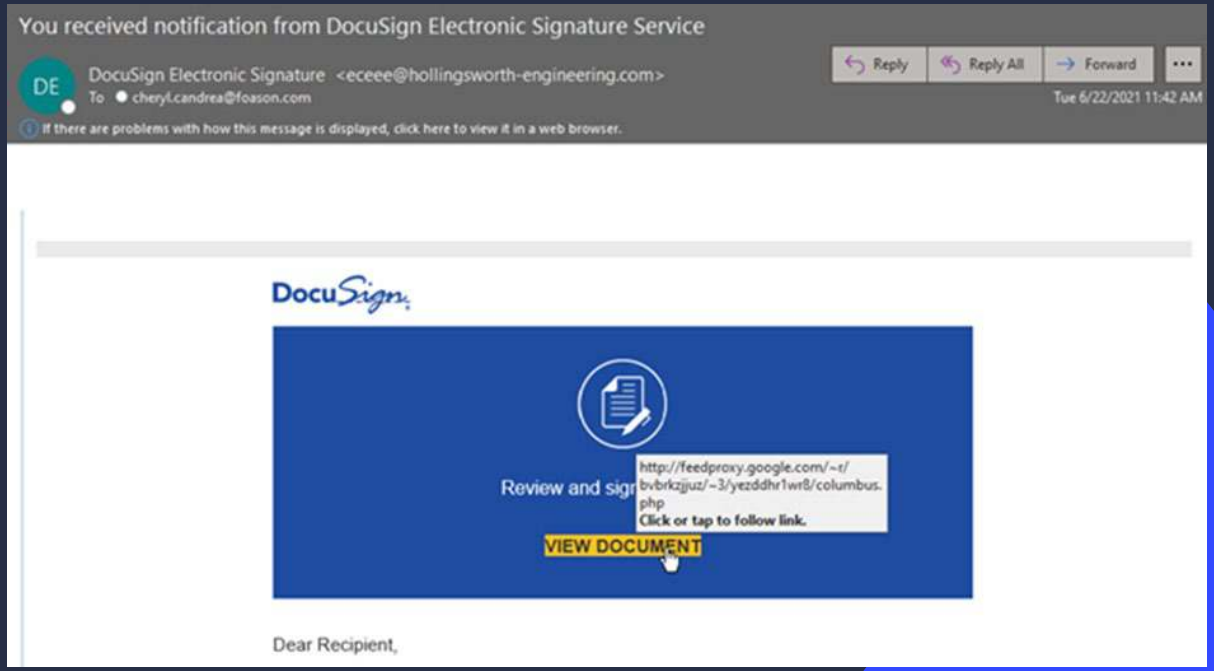




Living off the Land (LOtL) Phishing Attacks



Living off the Land (LOtL) Phishing Attacks



Remcos RAT -Tax Scam

zix

Request For Tax Service

KJ [redacted]Jennifer <postmaster@smarthomesfls.com>
To recipient

Reply | Reply All | Forward | ...
Tue 3/2/2021 1:35 PM

Tax-Document2.xlsb 46 KB | Image1.jpg 108 KB | Image2.jpg 101 KB

Good Day,

I would like to employ your tax services,Please take a look at the last page of the attached VERY carefully. I have about $250,000-$350,000 in income to myself personally and to my LLC that I have not yet paid taxes on. For about $80,000 of that there is no 1099 of any kind, it's purely me self-reporting. Do not count the 1099 from Square—I am including that amount in the self-reported income, as I explain. Very important not to double count that.

I am attaching all my existing tax documents for 2020, as well as my 2019 return (Due to the confidentiality of details Tax-Document Password: 2021).

NOTE: I have not yet received any tax document from Airbnb, but I listed the income on the last page. I have also not yet received the 1099 from the Federalist Society for my LLC ($20,000). You'll see there is a 1099 from them to me personally. There should be another one coming for the LLC.

Thank you—and please let me know if you have any questions! I know I will owe additional taxes this year, ugh...let's try to minimize as much as possible!

Thanks
[redacted]Jennifer

Security Tips

zix

Never reuse the same password on different services, if the service is compromised attackers will try that same password for others.

Implement a VPN for all remote workers but resist using a free VPN service as they often monetize your private data

Limit use of third-party services

Use end to end email encryption for any message containing confidential or personally identifiable information

Ensure your solution is capable of dynamically analyzing email attachments

Audit your email environment for O365 users our Security audit can provide critical insights

If there is any suspicion about a message or transaction, it never hurts to call the sender. Most will be glad of your security protocols in place to help prevent fraud

Security Tips

Attack the target

Using collected intel, launch attack for initial compromise

Evade and move

Hide presence as attacker conducts internal recon

Identify a target

Initial recon to select the weak target and determine how best to attack

Infiltrate the target

Once breached, establish an internal foothold

Complete mission

Using collected intel, execute mission goal

Security Tips

zix

Protect

Advanced Email Threat Protection
Multi-factor Authentication
Advanced Email Encryption

Detect

Security Audit
Threat Analysis Team / Tools
Data Loss Prevention Scanning

Respond

Threat Investigation / Analysis
Vulnerability Remediation
Backup and Recovery

Thank you.

Andrew Murphy
Director of Product Marketing

Questions?