zix | appriver

Global Threat Report
Full Year 2021

Introduction

Threat actors did not skip a beat in 2021. They continued to propagate attacks while constantly cycling through both new and old tactics. They were always revising and improving their approach to help improve their chances of subverting both security controls and the human factor. In this report, we will explore many of those tactics in detail.

The phishing landscape is ever expanding as attackers find new avenues for attack. Threat actors committing Business Email Compromise (BEC) attacks showed no signs of abating throughout the year. While their approach generally required a minimal amount of time and money investment, we saw them deploy some interesting new tactics. Those committing Living of the Land (LotL) phishing attacks continued their abuse of many of the legitimate services we had seen them using prior. However, they also added many new services to their arsenal and began chaining these services together within the same attack to enhance obfuscation. We also saw them employing the use of CAPTCHA technology to further obfuscate the true nature of their attacks. In addition, there was a significant uptick in call-center-based phishing attacks. These were far more prominent than in recent years and relied on phone-based scammers to deploy a bevy of threats. Phishing attacks targeting cryptocurrency assets were also on the rise this year with attackers finding new methods for defrauding investors.

Malware threats grew in both abundance and functionality. In January we saw a huge win for society as the Emotet malware was taken offline in a coordinated law enforcement effort. Shortly after, we saw other malware families attempting to fill the Malware-as-a-Service (MaaS) void that was left behind. While this was a welcome respite from the threat posed specifically by Emotet, it proved to be temporary. In mid-November Trickbot was observed re-sending new versions of Emotet. And just a few short days later we could see that Emotet had regained its foothold across the threat landscape. We also saw the emergence of a new malware dubbed SquirrelWaffle. We have seen it used relentlessly to target businesses since mid-September and it has been successful in leveraging vulnerabilities in Exchange servers.

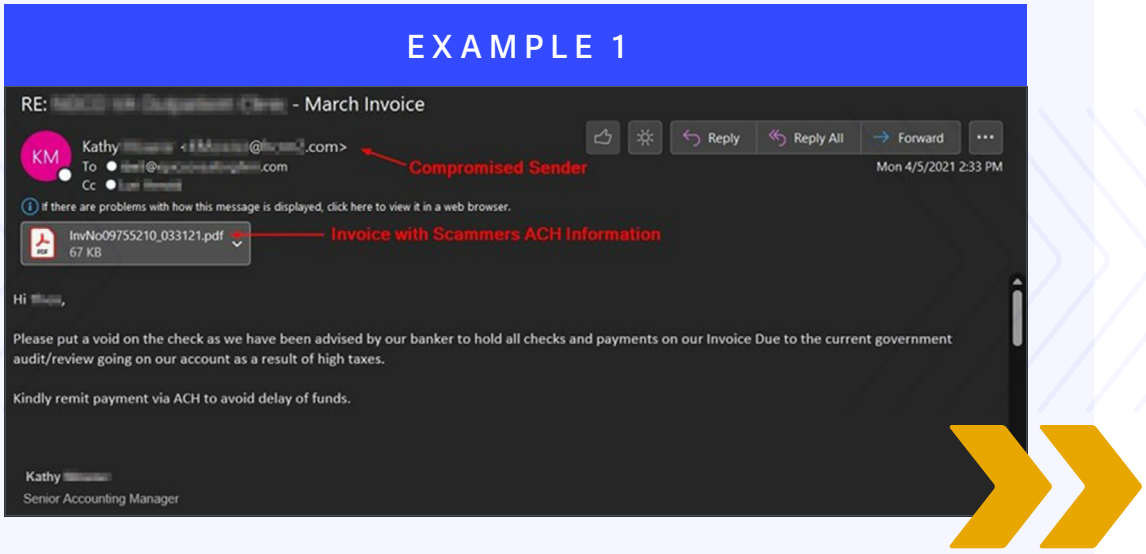
Like clockwork, threat actors were there to capitalize on world events with clever social engineering attacks. After supply chain attacks like Kaseya, we saw malicious actors sending emails posing as related security patches. As news unfolded surrounding global supply chain and shipping delays, we observed threat actors looking to leverage this situation in some clever phishing attacks. COVID also continued to prove fertile ground for many email attacks - especially with the emergence of the Omicron variant.

Business Email Compromise Attacks

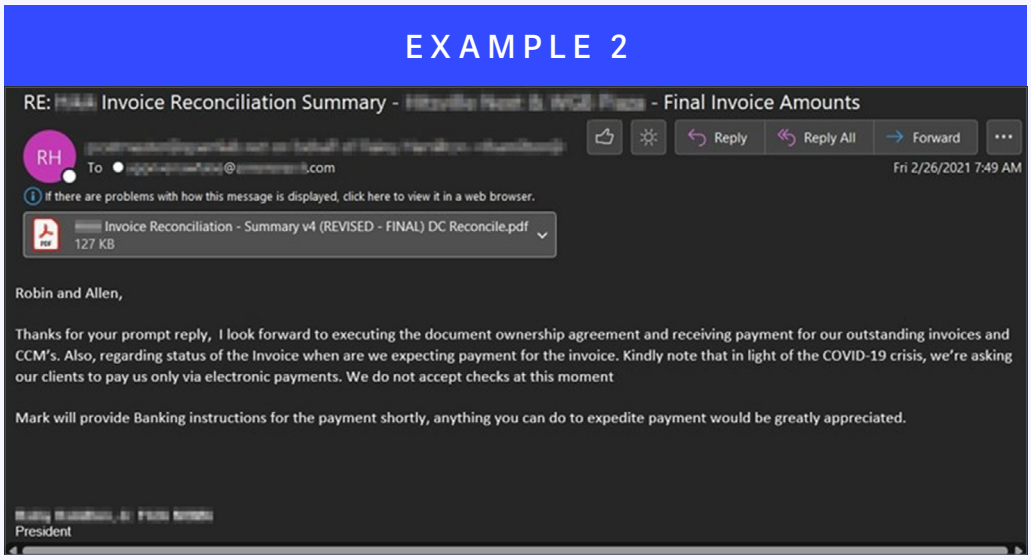
Business Email Compromise (BEC) attacks continue to be a favorite avenue of threat actors throughout 2021. The attacks require minimal time or money investment and can yield huge windfalls for the attacker. BEC attacks have also proven easier to get past layers of security solutions when compared to traditional directly attached malware attacks. While MaaS operations have increased, BEC attacks do not require the same level of technical knowledge or expertise. Attackers utilize a variety of different methods to achieve their end-goal—financial fraud. The most common versions we protect against usually begins with spear phishing emails designed to grant the attacker access to an account.

Once inside an account, the attacker monitors legitimate conversations and looks for an opportunity to insert themselves at the perfect time. They do this to redirect financial transfers and payments into their own account. To add the sense of legitimacy for the target, many times the attacker will register a similar domain to the compromised users to give the appearance that multiple people in the company are part of the transaction. If they are unable to do this in the account that they have compromised, then they pivot to another account by sending more phishing messages to the contact list of the compromised user. Using this method, the attacker will keep pivoting to gain access to an account which does handle monetary transfers.

Pictured below, this attacker has compromised a user and is attempting to change the payment method from paper checks over to ACH transfers. They have simply modified the original PDF invoice to contain their bank account information within attempting to steal almost $150,000 (USD).



In the next BEC attack example, the attacker has also stated they are not accepting checks for the invoiced amount in light of the COVID-19 crisis. They state another person in the email thread will provide banking instructions for the payment shortly, however this attacker has either compromised two users or setup a similar domain from which they will send their payment information. In this attempt they were aiming to steal $250,000 (USD).

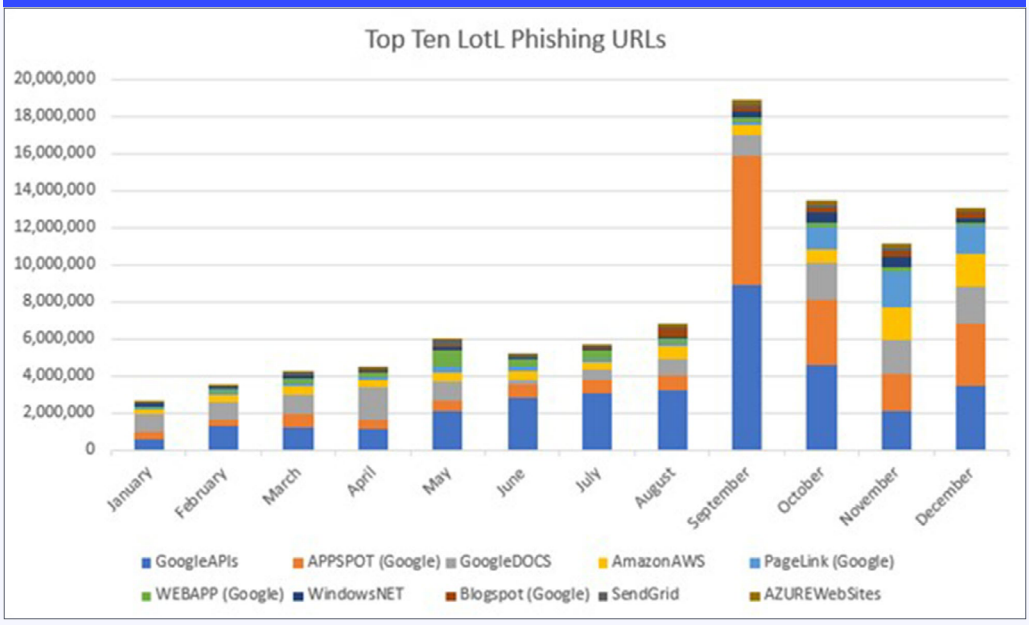


Chained Living Off the Land (LotL) Phishing Attacks and other obfuscation

LotL phishing attacks continue to proliferate as they offer threat actors the benefits of using legitimate services for illegitimate purposes. In addition, it is much easier to conduct attacks from the legitimate platform as little to no extra infrastructure is needed. We see some of the attackers routinely rotate through different platforms over time to keep defenders on our toes.

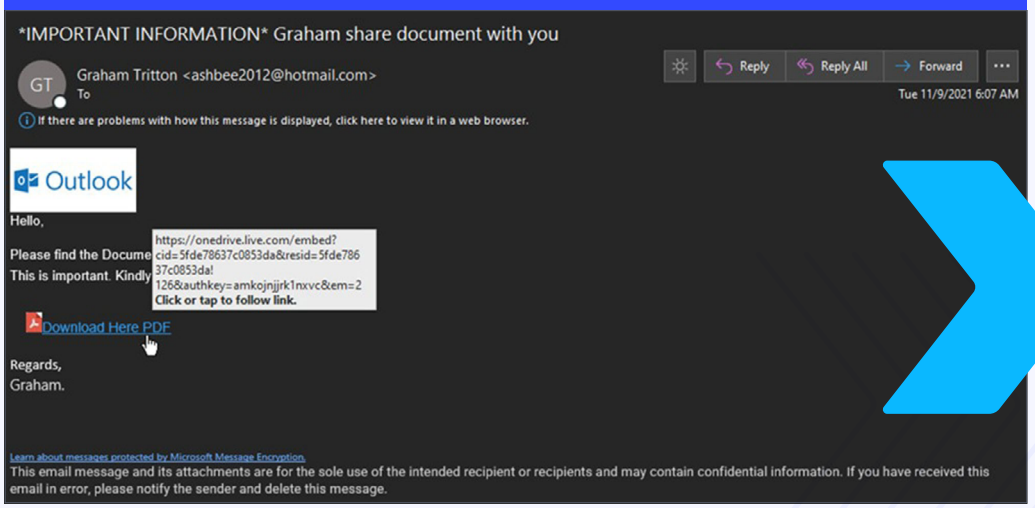
The chart below depicts trends throughout the year for the top ten services most abused to disseminate LotL phishing attacks. As you can see this method has become more prevalent throughout the year. In addition, threat actors have also embraced the tactic of chaining several of these services together within the same attack to better their obfuscation. We will cover some examples of this in the sections below.

TRENDS

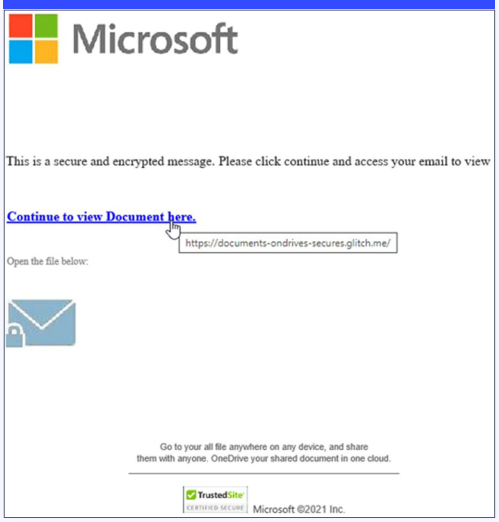


Threat actors continue to masquerade as encrypted messages in a multitude of formats with varying levels of sophistication. For the example below, attackers have done just that while maintaining brand cohesiveness with their OneDrive theme. This message is disguised as a Microsoft encrypted message.

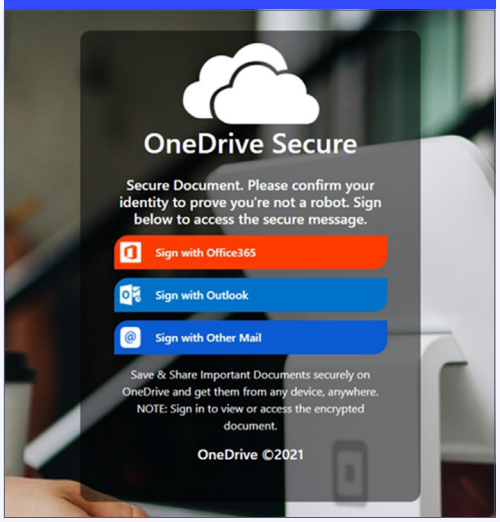
EXAMPLE 1



Once clicked, the OneDrive link hosts an image lure that points to Glitch (glitch.me), a legitimate service being abused by LotL threat actors.



If the user proceeds, they are taken to the credential harvesting site hosted on Glitch with a Microsoft OneDrive theme.

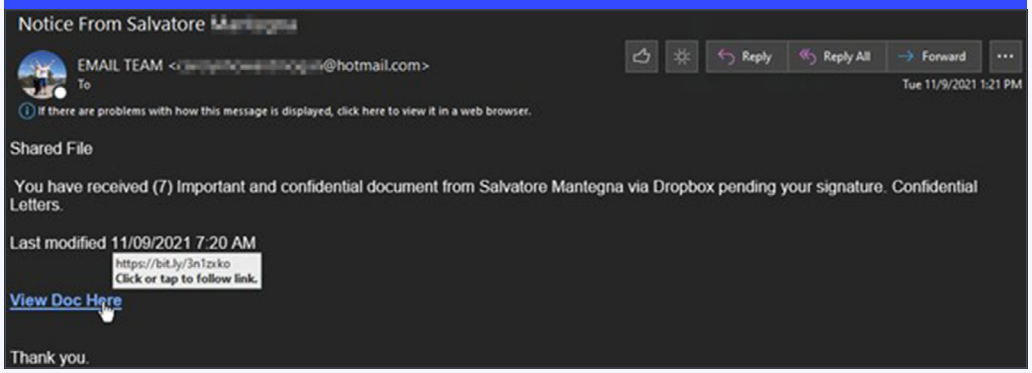


For better or worse, URL shorteners are extremely prevalent in email traffic. They are a convenient way of shortening lengthy URL's by providing a cleaner presentation while providing click analytics. However, they have also proven a useful tool for threat actors as they heavily abuse URL shorteners to disguise link destinations for the purpose of harvesting credentials and distributing malware. Clicking on a shortened URL can take the end user through multiple redirects before arriving to their destination.

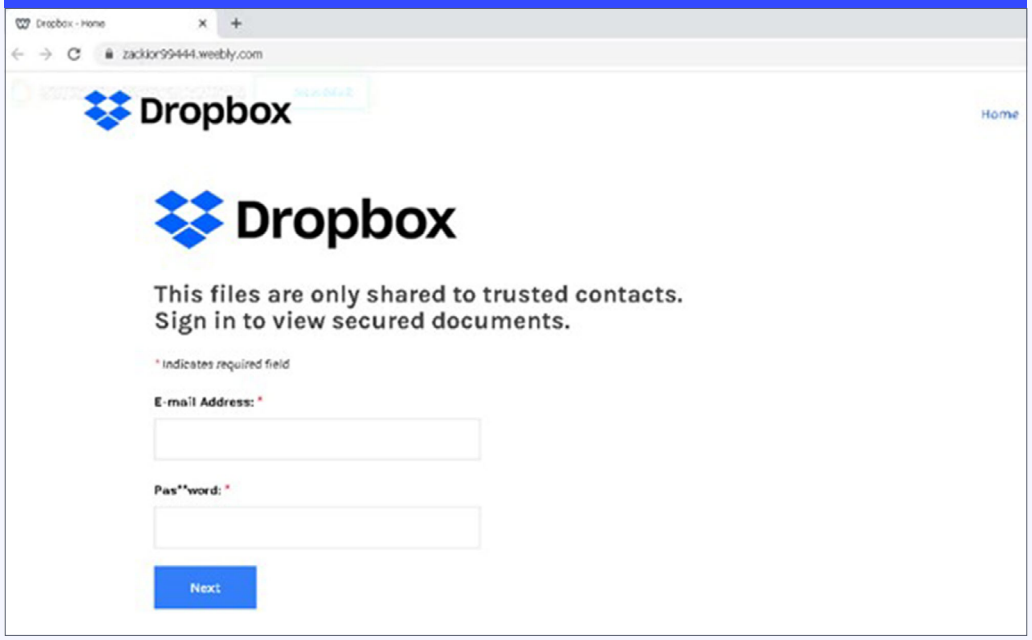
Below are commonly abused URL shorteners to keep an eye out for:

- Bit.ly
- Cutt.ly
- Tinyurl.com
- Is.gd
- Ow.ly
- S.id
- Bit.do
- U.to
- Rb.gy
- Rebrand.ly

EXAMPLE 2

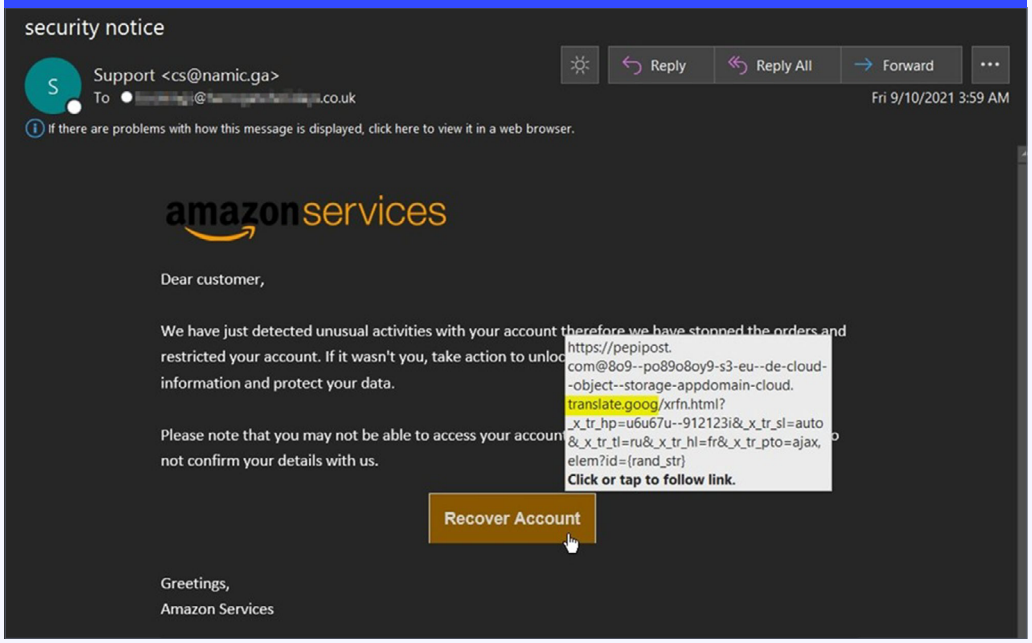


The bit.ly link above redirected to this Dropbox-branded credential harvesting page hosted on Weebly, a heavily abused free website builder.

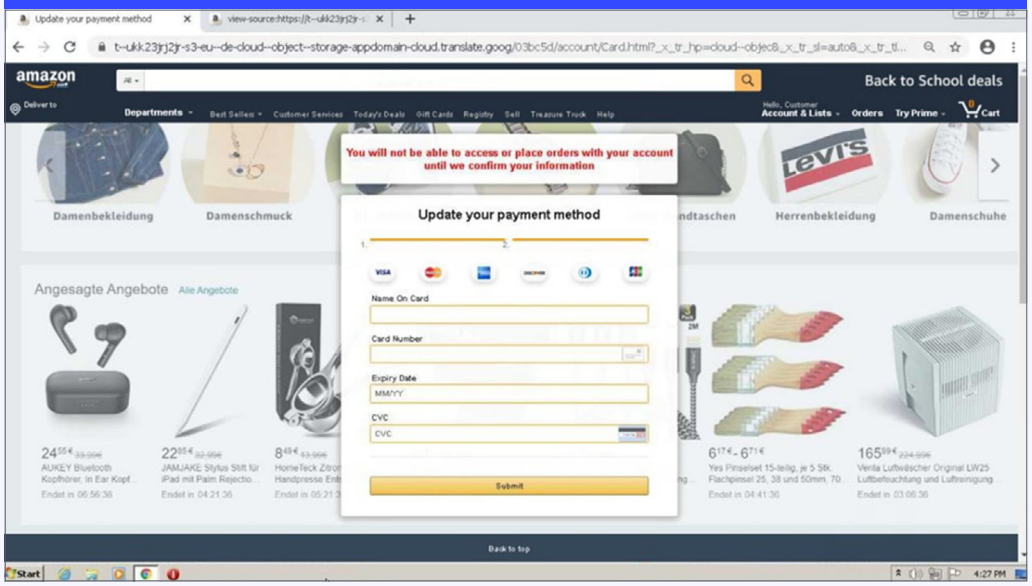


An Amazon-themed phishing attempt we captured in September had an interesting twist. It used a Google Translate root of translate.goog to help obscure the remote appdomain.cloud (IBM Cloud) link used to host the attack.

EXAMPLE 3

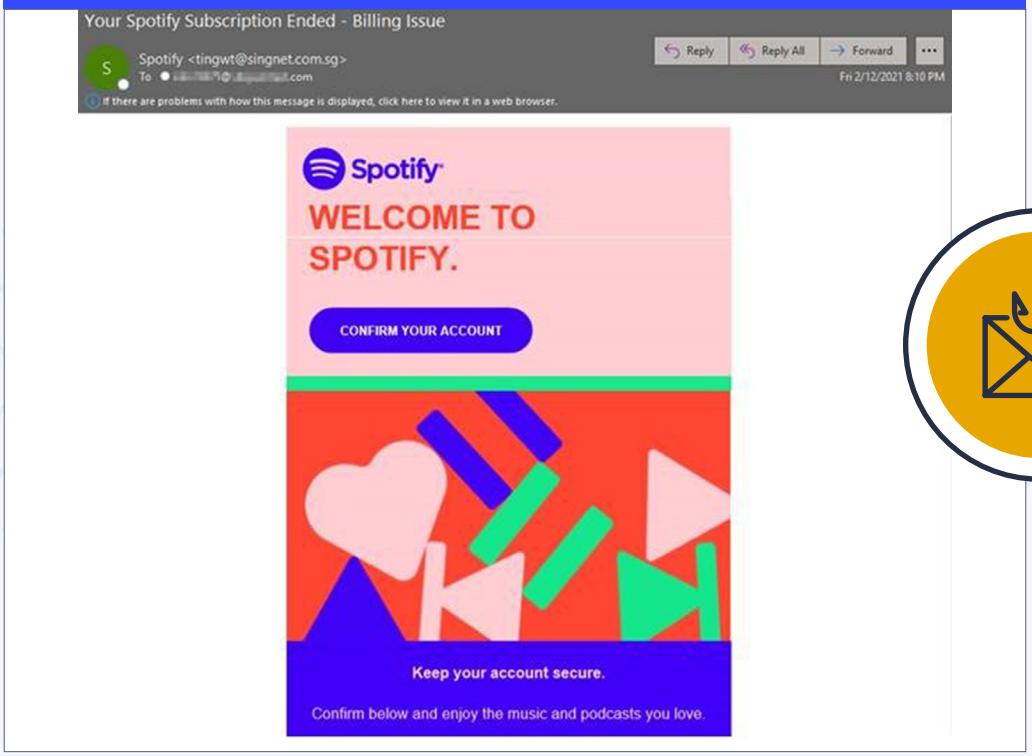


Upon clicking the link, it still appeared as the Google Translate root domain in their browser, however, it loaded the content directly from appdomain.cloud platform. This threat actor initially went after the user credentials with this attack. If credentials were entered, they attempted to have the user "update their payment method" by inputting their credit card details. This attack tried to knock out two birds with one stone by combining credential harvesting and direct solicitation of credit card information from victims, a trend that has been on the rise lately.

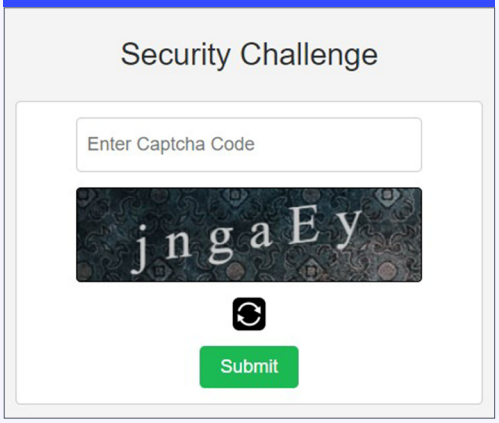


In 2021, we are seeing more Captcha live-user technology incorporated into phishing attempts. In February we observed a Spotify phishing campaign using this technique. We anticipate seeing this used more often since the presence of live-user verification methods helps attackers hide the content of their landing pages from web scanning bots that might otherwise identify it as malicious.

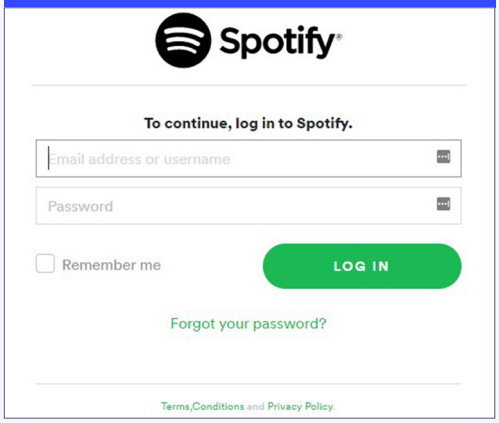
EXAMPLE 4



Clicking on the "CONFIRM YOUR ACCOUNT" link leads to the below Captcha security challenge that must be correctly entered to proceed.



Once the captcha is completed the user is directed to a Spotify branded credential harvesting page.



Tech Support Scams

Beginning in April social engineers ramped up bogus billing renewal notices purporting to be from Microsoft, McAfee, Norton, Geek Squad and more. These attackers claimed that a service subscription ended, and that the victim's card had, or was about to be, charged for an automatic renewal. In these attacks the "payload" was the included phone number. These scammers relied on social engineering to coerce victims into installing remote session software, gathering personally identifiable information (PII), or installing malware under a remote assistance guise.

[PRO-TIP]: Calling a number included in a suspicious email is never a good idea. We suggest navigating directly to the company website and contact the number listed there. It is important to remember that no legitimate company should ever require you to download remote access software so they can control the computer just to uninstall their software and process

EXAMPLE 1

Your subscription has been renewed

JY Jiang yanlin <yanlinjiang2@gmail.com>
To [redacted]

Reply | Reply All | Forward
Tue 9/21/2021 10:30 A

GEEK TECH SQUAD LLC
Online Technical Support

Auto Renewal Amount: - $597
Subscription Date: 09/20/2019
End Date: 09/21/2021
Product Code: #49802
Product Name: Network Security
Renewal Status: Auto Renewal
Consumer ID: 11478965

Dear Consumer,

We hope you are doing great; it's our pleasure to serve you as our registered customer. We have a new network security update ready for installation.

As per the record, your plan will be auto renewed and card will charge $371.23 USD.

Call us on toll-free for any concern +1-844-653-4968 or +1-866-259-0223

Please let us know if you have any questions or concerns, Have a great day!

Thank you for choosing Geek Squad®.

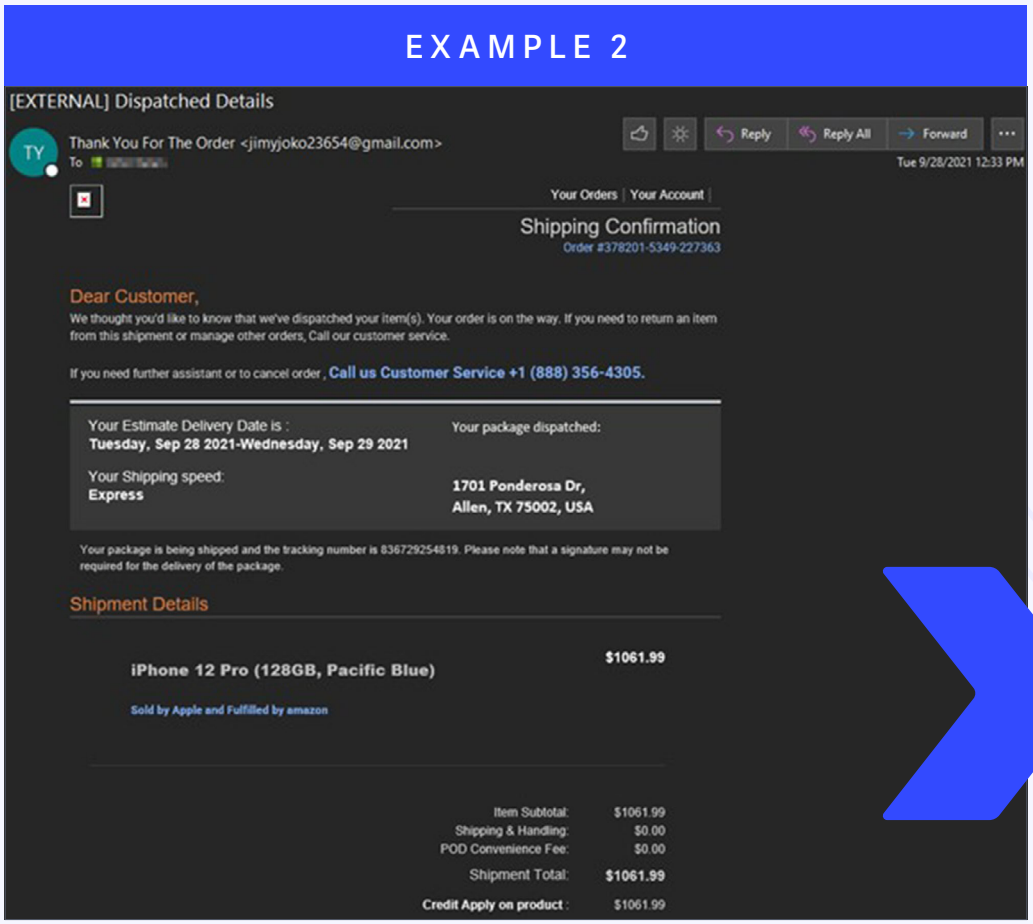
Regards,

Premium Virtual Support

Geek Squad®

+1-844-653-4968

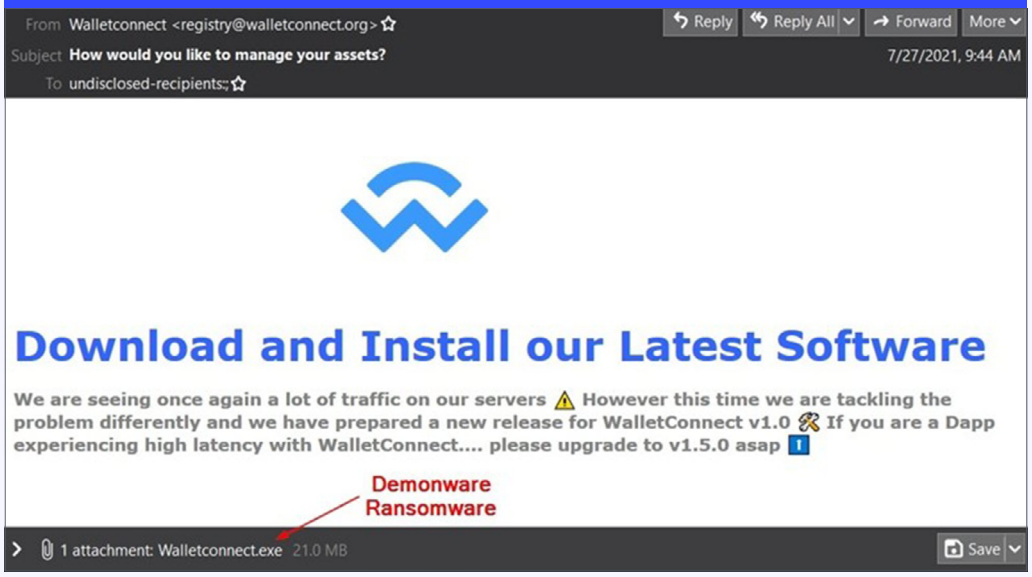
The scammers didn't just stick to billing renewal notices. Later they began to state that a large purchase, such as iPhone or Samsung mobile device, was made and being shipped to the victim. PayPal, Walmart, & Amazon were the primary themed services involved in this variation of the scam.



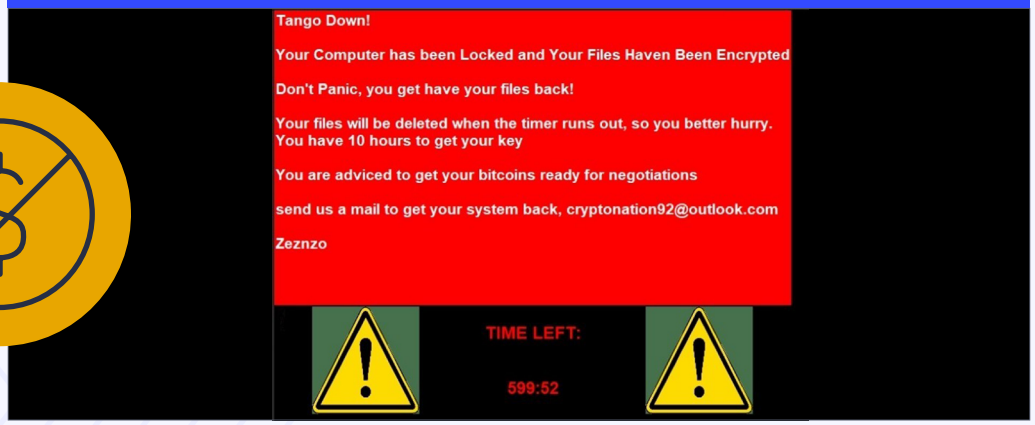
Cryptocurrency Scams

The most enterprising threat actors chain attacks after initial access from a Remote Access Trojan to a Banking Trojan then a final Ransomware or Crypto jacking payload. However, we have captured an increase of directly attached ransomware executables this year. One attack we blocked posed as a software update for Wallet Connect, "an open-source protocol for connecting decentralized applications to mobile wallets with QR code scanning or deep linking."

EXAMPLE 1



Upon running the attached executable, the recipients' files were locked with then a 10-hour countdown timer began. The victim is urged to contact the ransomware actor via email with bitcoin ready for negotiations. Unfortunately, anyone could conduct this attack as the proof-of-concept code is located on GitHub.



Attackers continue to come up with creative ruses to defraud cryptocurrency investors via phishing attacks as well. One recent Coinbase-themed message was just so overly too good to be true that it caught our eye. It promised 100% returns in 48 hours. Naturally, we had to look at this attached "100%-SmartContract-Investment-Registration.pdf."

EXAMPLE 2

Earn 100% Returns on your Crypto within 48 hours

Coinbase <taxifunkrgbg@t-online.de>
To Recipients

Reply | Reply All | Forward

Fri 11/12/2021 9:28 AM

100%-SmartContract-Investment-Registration.pdf
119 KB

Coinbase Smart Contract Investment

Hello there,

Earn 100% returns on your Bitcoin or Ethereum within 48 hours from our Smart Contract Investment program. Only the first 100,000 investors that will register and invest early will have the opportunity to take part in this massive investment giveaway.

Hurry! Register, invest via the secure registration attachment in this email and wait for your wallet to be credited with your total invested amount and the additional 100% returns within 48 hours.

Coinbase Team
This is an automated message, please do not reply.

Once opened, the PDF served as an intermediary jump page by social engineering the user to click a link and be redirected elsewhere to "Register to get started". Using jump sites or intermediary documents like these is a favorite tactic of threat actors. It allows the attacker to easily switch up the links in these files as threat feeds or email filters start picking up on them while increasing the chance that the ultimate destination will not be recognized as quickly by threat feeds or taken down.

100-SmartContract-Investment-Registration.pdf - Adobe Acrobat Reader DC

File Edit View Sign Window Help

Home Tools 100-SmartContract... ×

1 / 1 75%

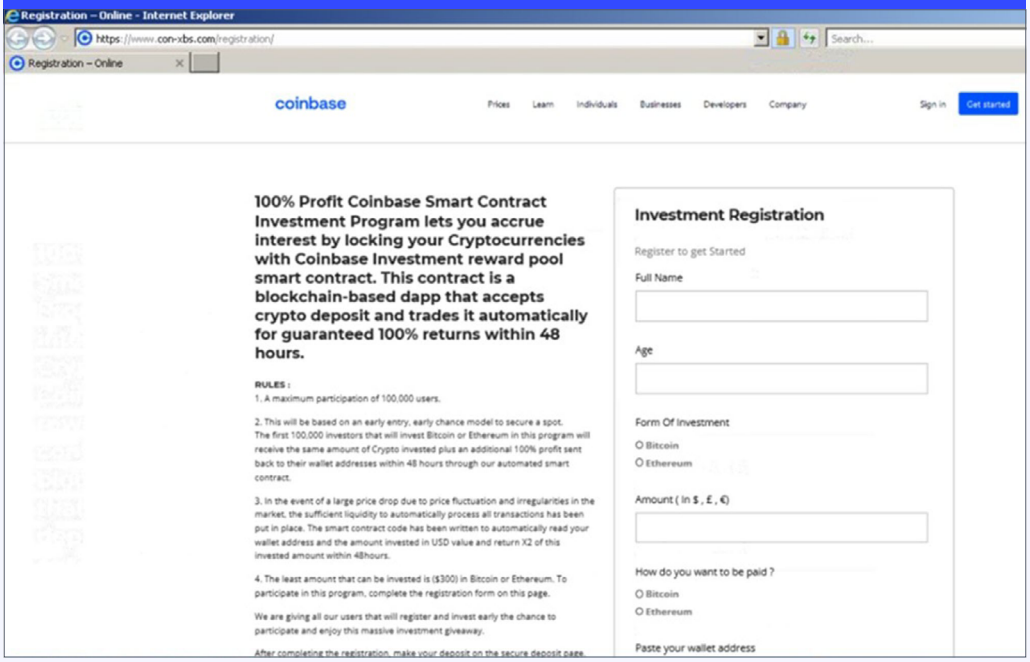
coinbase

PDF Adobe

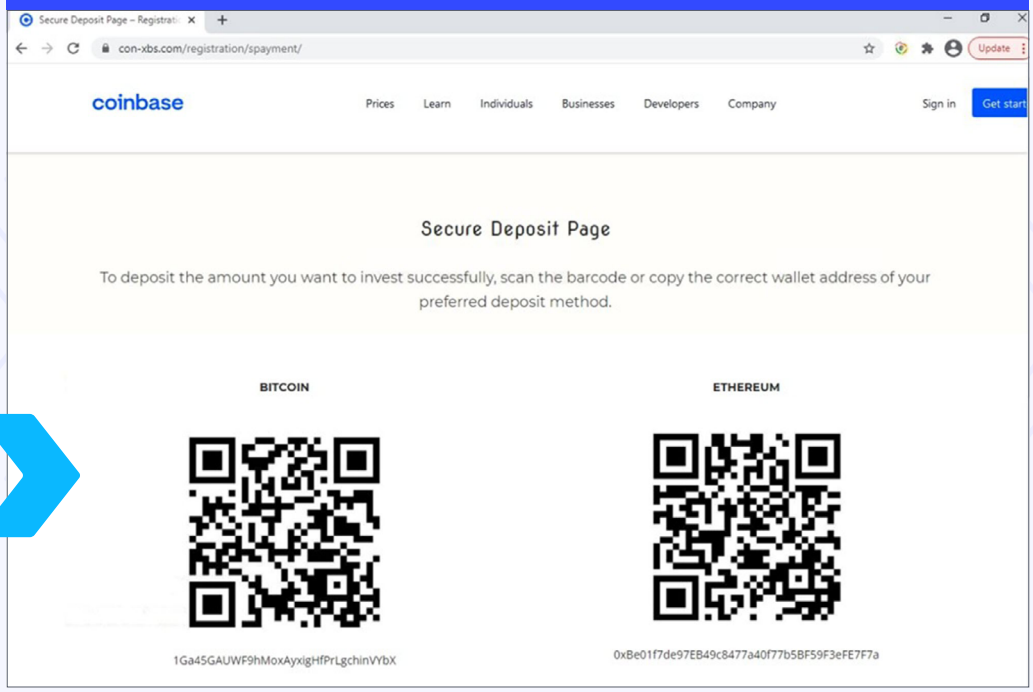
Investment Registration File

Register to get started

After clicking the link in the PDF, we were redirected to a site that cloned quite a bit of Coinbase's real site while further elaborating on the scam. The opening page asked for seemingly innocuous user information leading the victim on to believe they were going to realize the promised returns without attempting to raise too many red flags.



Digging deeper, we found the wallet address/QR deposit page where the unassuming victim would, upon depositing funds, be scammed out of their Bitcoin or Ethereum cryptocurrency. Initially, there were no cryptocurrency transactions associated with these wallets. While writing this threat update, we checked them again and it appears the Bitcoin wallet is being used for mixing/tumbling activity which could help to anonymize legitimate transactions or launder illicit funds.



Crypto jacking, the unauthorized use of a victims' system resources to mine cryptocurrency, continued to occur this year as cryptocurrency valuations rose to all-time highs. One of the attacks we captured posed as a "new order evaluation" with an Excel attachment. However, if executed, this file would load XMRig Monero mining software onto the victim's system.

EXAMPLE 3: XMRIG CRYPTO JACKING ATTACK EMAIL

New Order Evaluation

sales9@resinchemicals.com
To info@[redacted].com
Cc aykinalv@mail.ru

Reply | Reply All | Forward

Mon 5/10/2021 5:05 AM

Order Schedule.xls
61 KB

Dear info,

Well received for your quotation sentr from info@[redacted].com and my customer also interested. So,Let me ask only one question. How long can take the duration time for the product to arrive Yangon Port, Myanmar from your factory (Factory-Shipping-Yangon Port) if I drop the order please ?

Best Regards,

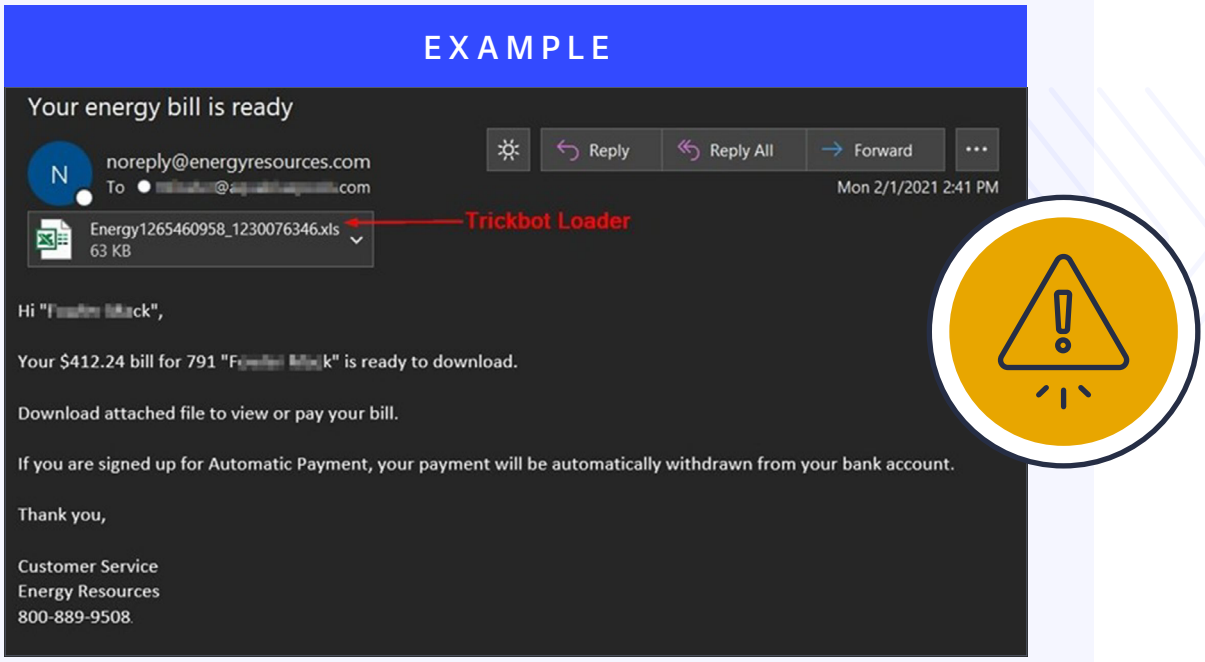
Aung Kyaw Lwin
Director
KYAW_APEX MACHINERY
Phone: +95 1 555 797
Mobile:+95 9 775 755 523
E-mail: aungkyawlwin@kyawapex.com

Top Malware Threats

Trickbot

Trickbot is a modular banking Trojan primarily designed for financial theft, and it utilizes a variety of malicious capabilities. It was first spotted in 2016 as a banking trojan but has since evolved into a modular platform capable of lateral scanning and movement using vulnerabilities to increase the possibility of compromising further victims. It is also environmentally aware, which helps it evade anti-virus, sandbox, & virtual machine detection. Additional malicious dynamic link library modules include process hollowing code-injection, keystroke grabbing, start-up persistence, scraping address book contacts, credential theft via Mimikatz, screen-locking, and worm functionality with lateral movement via MS17-010 using SMB / Eternal exploits.

Last year its developers had also worked on a persistence capability which infected the UEFI firmware of devices that were not write-protected. This allowed the malware to survive a hard drive reformat or replacement since the malware instructions were in the low-level bootup firmware. In addition, it has survived previous takedown attempts which ultimately increased resiliency of the botnet. All capabilities considered, Trickbot is a fully capable crimeware delivery platform with connections to both state-sponsored attackers and criminal ransomware groups. The partnerships the operators have forged across the cybercrime world extends well beyond any borders and remains one of the top cyber threats.



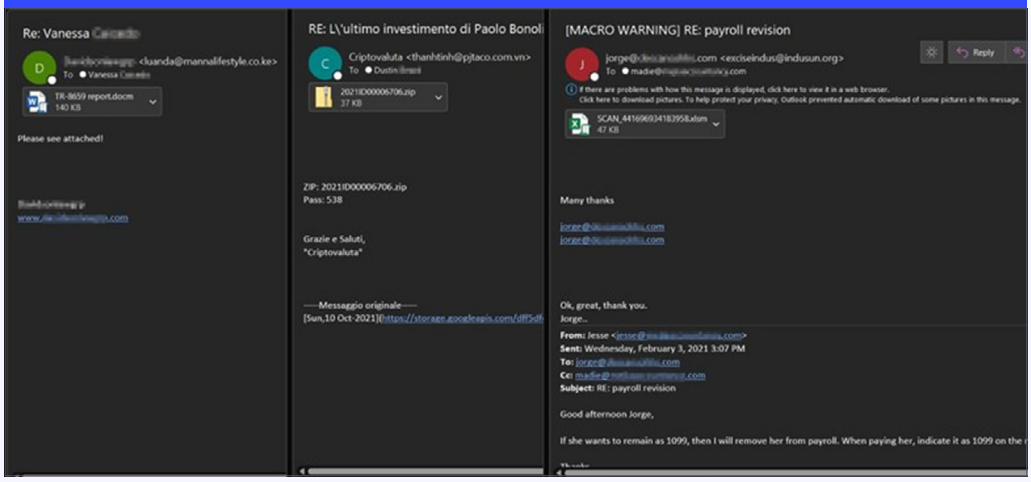
The Return of Emotet

The modular Emotet trojan has been a top nemesis for both email defenders and incident responders since 2014.

Emotet is one of the most advanced, professional, and sustained Malware-as-a-Service (MaaS) operations. Initially it began operating as a banking trojan but over time expanded its scope to act as a loader for distributors of other malware families to leverage. Last January, law enforcement cooperation efforts across the globe were fruitful enough to take control of command-and-control infrastructure and arrest some of the operators. Afterward, they initiated uninstallation of the Emotet trojan from compromised systems. Afterward, it was all quiet on the Emotet front. However, we predicted that it was likely we would see the group return at some point. Unfortunately, that prediction came true.

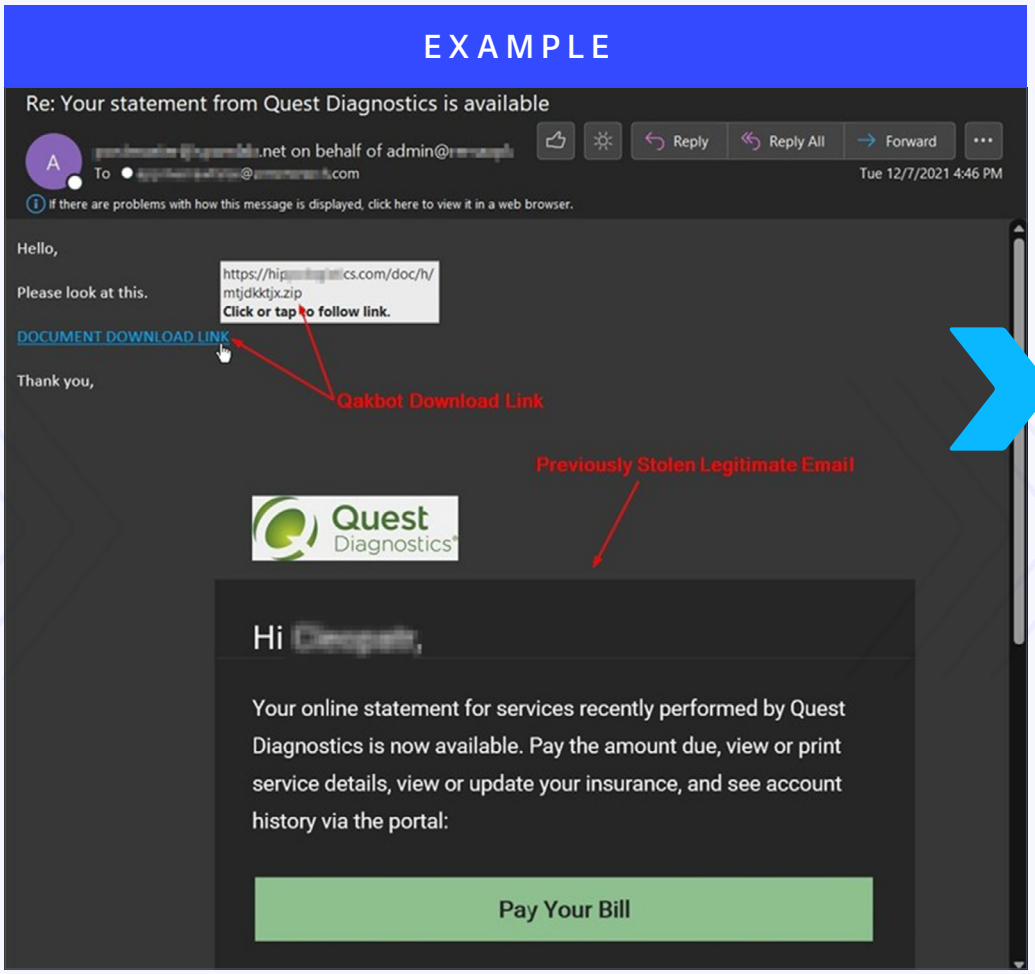
On November 14th, Trickbot was observed re-seeding new versions of Emotet malware onto compromised systems. It has been reported the Conti ransomware group (formerly Ryuk) orchestrated the return of Emotet to help fill the void left for initial access into compromised systems. Emotet email campaigns typically use multiple attack methods with many running concurrently distributed via separate botnets known as Epoch 1-5 by security researchers.

EXAMPLE: EMOTET EMAIL



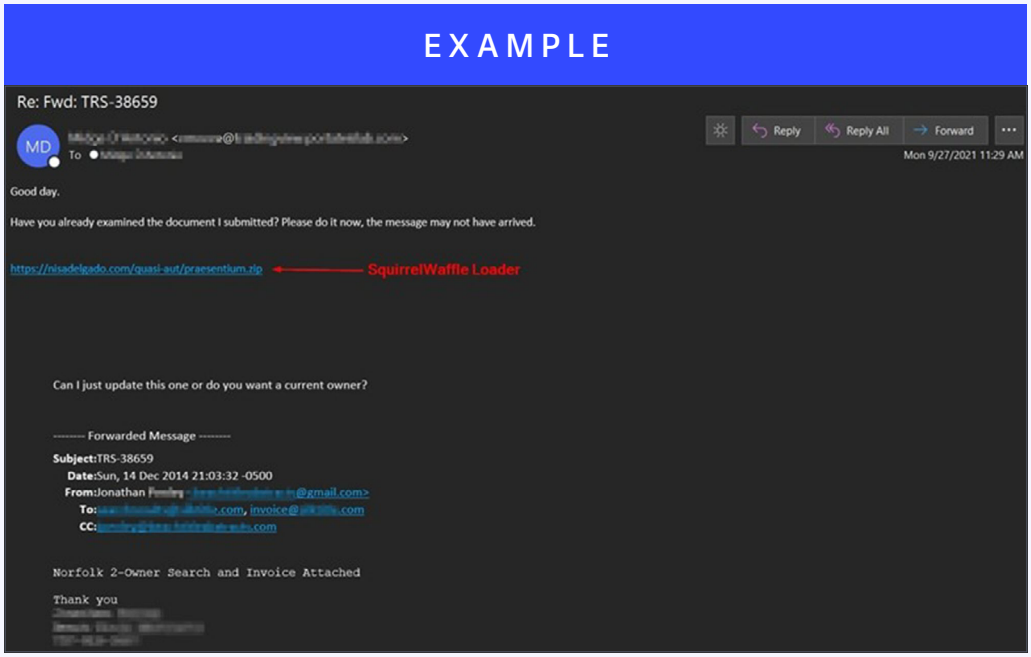
Qakbot

Qakbot is another highly capable banking trojan which has benefited from cooperation with Emotet & Trickbot threat actors. While Emotet was inactive, Qakbot filled in some of the MaaS gaps to provide threat actors the initial foothold into systems before dropping additional payloads. The follow-up payloads, such as Cobalt Strike, facilitate lateral movement and privilege escalation attempt for the threat actors. This could eventually lead to a ransomware deployment in compromised networks.



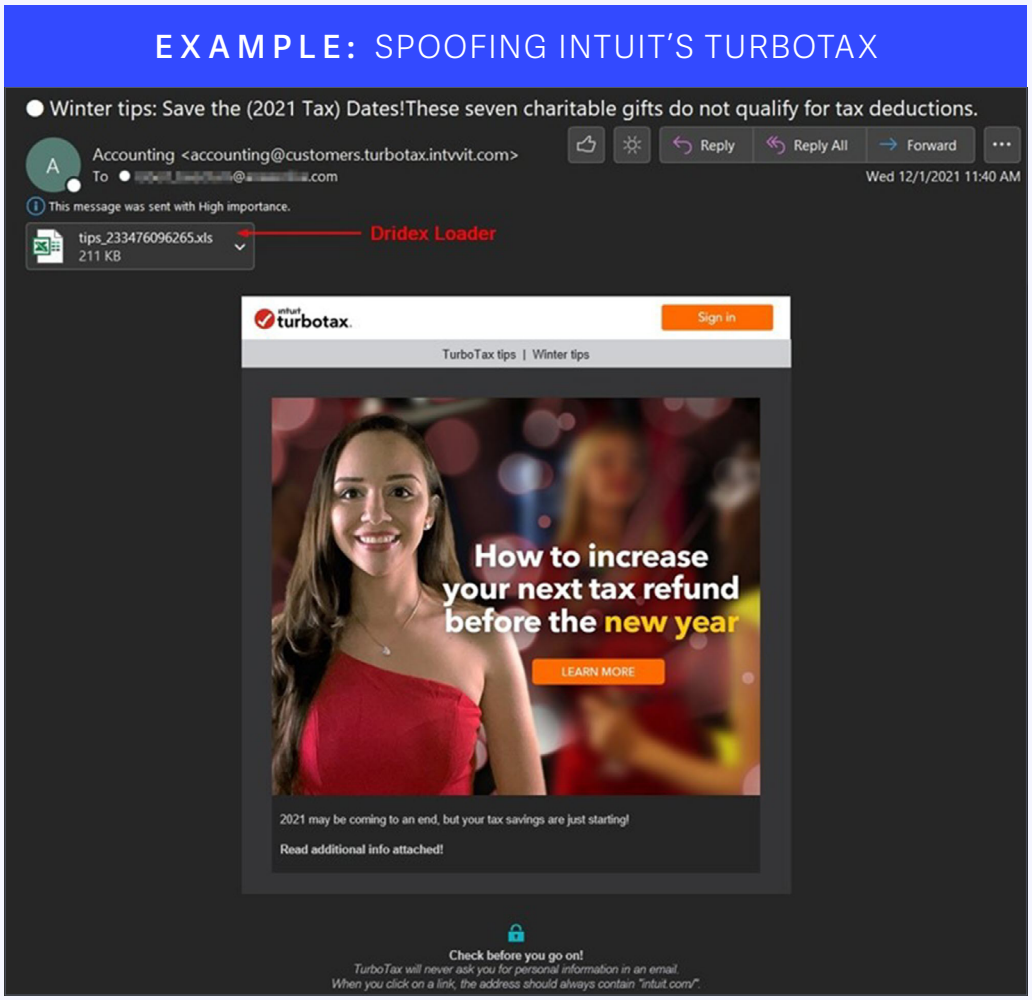
SquirrelWaffle Emerges

SquirrelWaffle was a newer trojan on the scene and was one of the top threats targeting customers since mid-September. Follow-up payloads also included QakBot or Cobalt Strike beacons which may lead to a ransomware deployment. SquirrelWaffle also spread across Exchange Servers via exploiting vulnerabilities that provide the attacker remote code execution capability. Once access was obtained, victims' emails were exported via exchange web service which allowed the attackers to respond to the victims' previous legitimate conversations.



Dridex

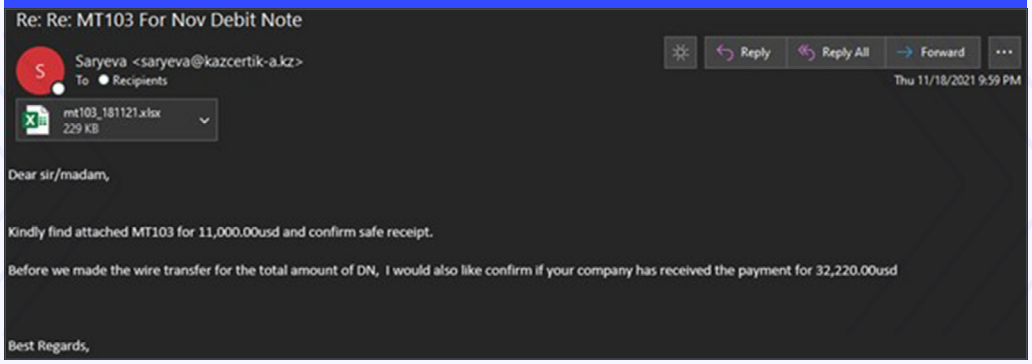
The Dridex banking trojan was the single highest volume malware strain we captured this year. It was distributed by different affiliates, although the Cutwail botnet accounted for the bulk of its volume. The affiliates campaign themes vary widely. However, bogus invoices or purchase receipts (as Excel attachments) are the favored tactic. For high-value targets, a ransomware payload may be dropped after the initial Dridex infection, thereby making it one of the most dangerous malware strains we captured.



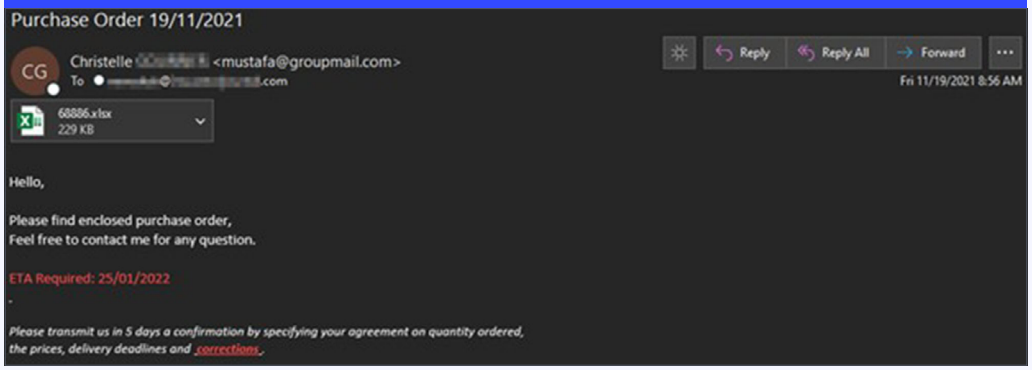
Info Stealer Spotlight — Formbook & Lokibot

Often overshadowed by the banking trojans, Formbook & Lokibot info-stealers have consistently been utilized for targeting customers every year, this year being no exception. Formbook has been around since 2016 but was recently upgraded this year. This upgrad helped it better evade detection and analysis by researchers along with utilizing CVE-2021-40444, a newer Office365 vulnerability vs the previous version utilizing CVE-2017-0199. The threat actors sending these stealers often run very similar campaigns in parallel to maximize success. Their malicious Excel files often contain an encrypted package attempting to obfuscate the payload within. Both trojans have very similar capabilities to include harvesting usernames, passwords, cryptocurrency wallets, and other credentials.

EXAMPLE 1: LOKIBOT



EXAMPLE 2: FORMBOOK

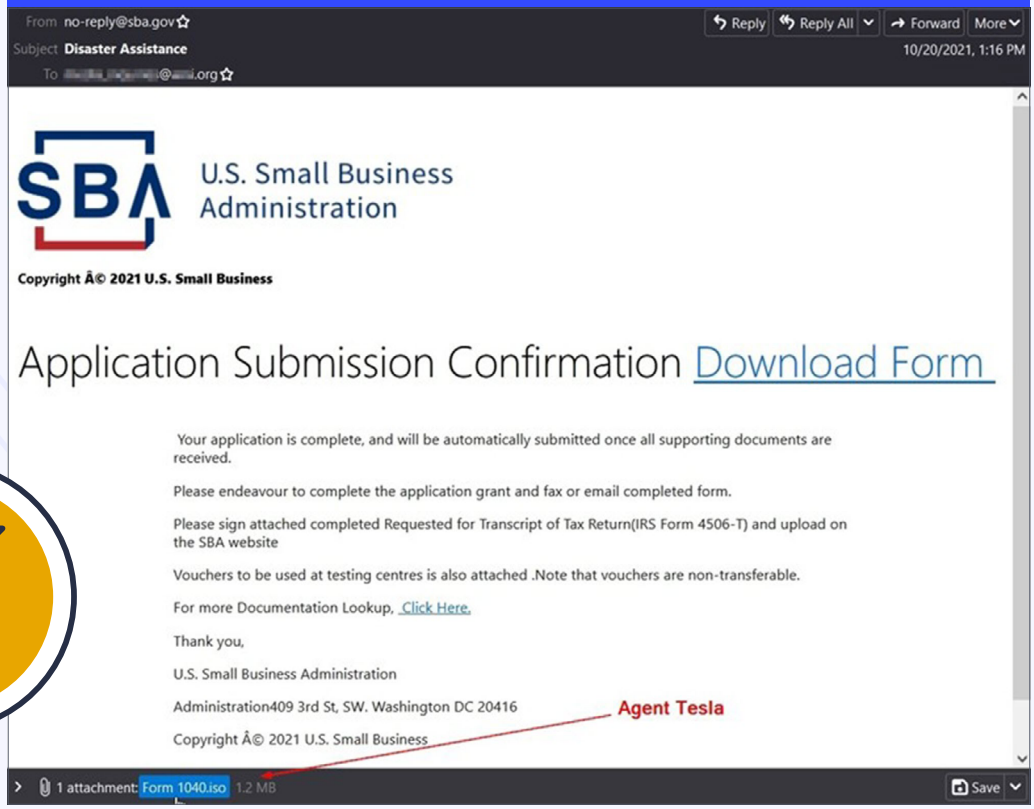


Remote Access Trojan (RAT) Infestation Continues

Synonymous with 2020, this year was another huge year for Remote Access Trojan (RAT) attacks. They provide the perfect foothold into compromised systems to allow the attacker to gain access and maintain persistence. There are a variety of capabilities they offer depending on the particular RAT. However, most offer the core ability to monitor users, gather credentials, control the system, and drop additional payloads.

Over the past few years, cybercriminal groups have been increasingly efficient at maximizing profit from every compromised system. Many follow the typical pattern of dropping a remote access trojan first, banking trojan second, then ransomware as the end-stage attack. Some criminals would also offer RAT compromised systems for sale so any enterprising threat actor could directly buy access for whatever their end goal may be - data and credential theft, ransomware, crypto jacking, etc. This differs from state-sponsored attackers who are primarily interested in gathering trade secrets and data intelligence, though system sabotage cannot be ruled out. The most common RATs targeting customers this year were Agent Tesla, NJRat, Nanocore, Netwire, Remcos, Adwind, BitRAT, Ave Maria, AsyncRAT, and LimeRAT.

EXAMPLE 1: AGENT TESLA RAT ATTACK



EXAMPLE 2: REMCOS RAT

Appraisal Loan Report.

CP [redacted]@appraisal-[redacted].com
To [redacted]s@[redacted].com

Reply | Reply All | Forward | ...

Mon 4/19/2021 8:59 AM

Appraisa-reportl11002275444900.zip
688 bytes

Dear [redacted].

An independent appraisal company has performed an appraisal valuation on your home. We have received a copy from the Appraisal Management Company, and a copy of the report is attached here for your records.

By sending you this report, we are also required to include for you the FAIR (FNMA Appraisal Independence Requirements) disclosure and information below. If you have any questions, please contact us.

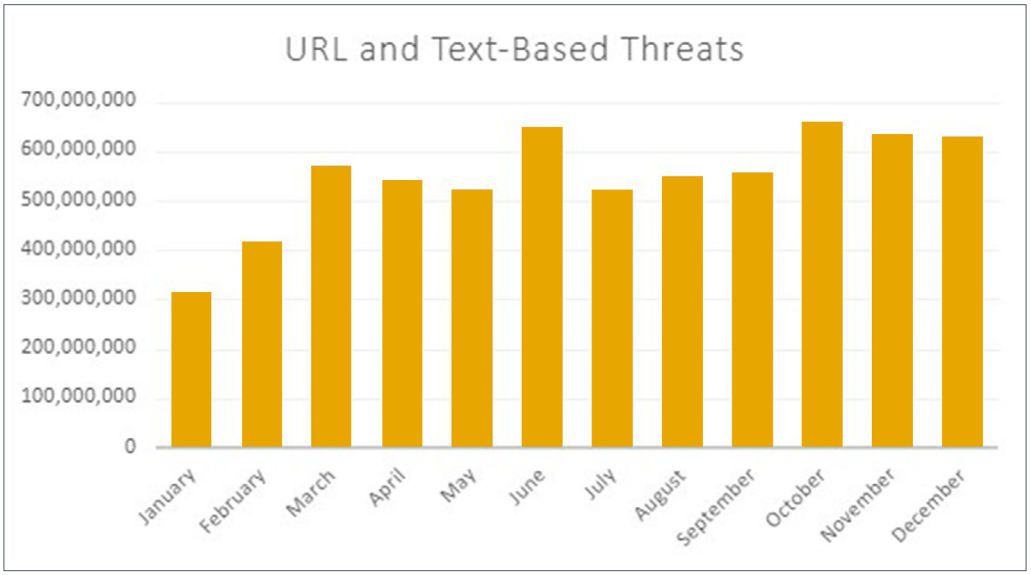
Please note: Because this email is auto-generated, you may have received the report before I've had a chance to review it in its entirety, but I will contact you soon to review the next step in the process.

FNMA Appraisal Independence Requirements(FAIR), Appraisal Delivery: Please find enclosed a copy of the appraisal report(s) that will be used in connection with your mortgage loan application. The enclosed appraisal report(s) was prepared for our use in evaluating the collateral used in the loan transaction for which you have previously applied. This appraisal should not be relied upon by any other person or entity, or for any other reason. No representation or warranty of any kind is implied.
Multiple appraisal reports may be included herein if such additional reports were required to evaluate your property and overall loan application or if a review appraisal was necessary in addition to the originally ordered appraisal.

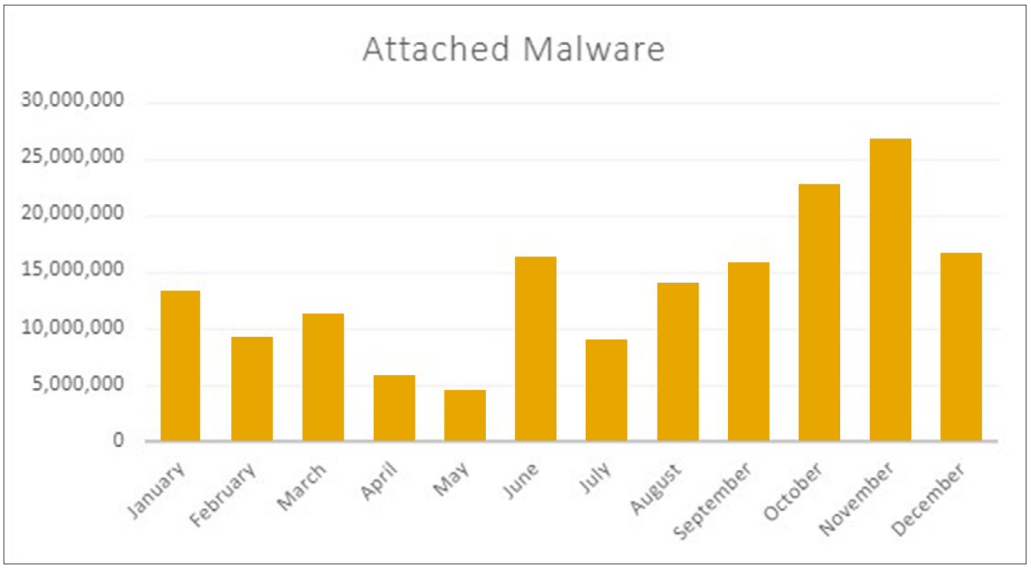
Sincerely,
[redacted].

Threat Metrics

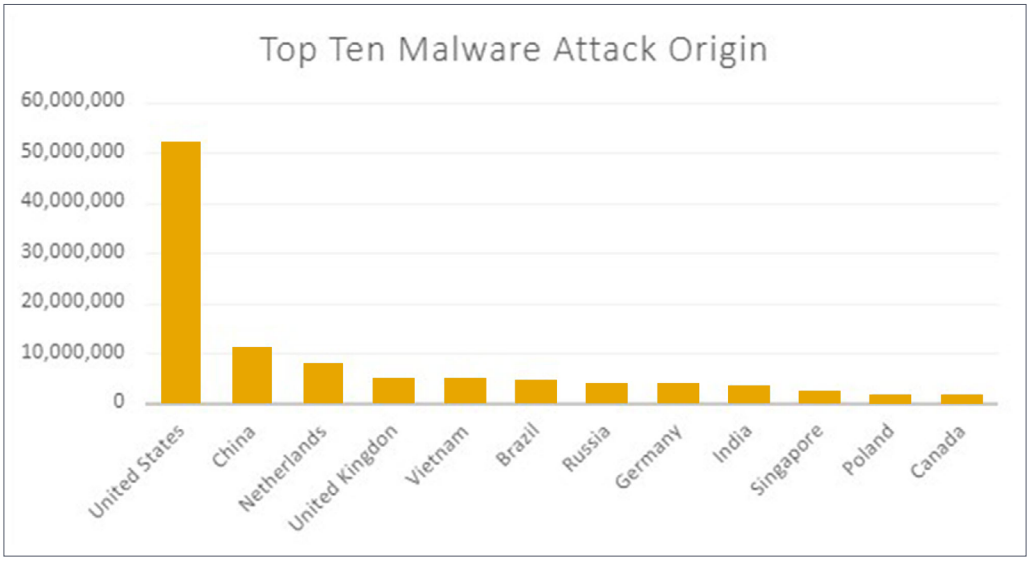
Overall email threats were on an upward trend throughout 2021. We quarantined over 6.5 billion email threats throughout the 2021, which was a 12.5% increase over last year.



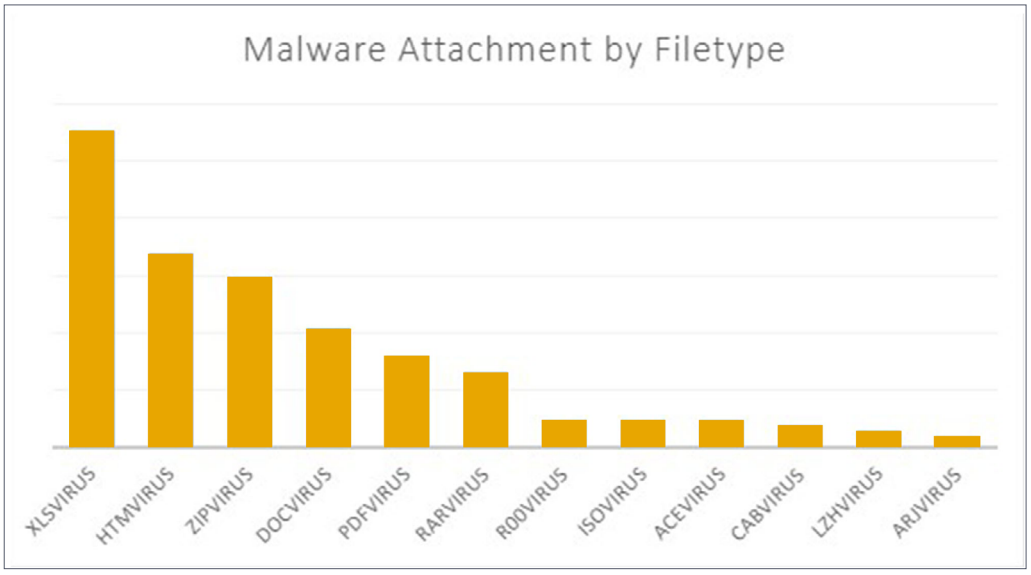
Emails with directly attached malware trended down throughout the first five months of 2021 before rebounding in June, then continued to surge throughout the end of 2021. In all, we quarantined over 165 million messages with malicious attachments through the first half of the year.



The US was the most common point of origin for emails with malicious attachments. Below are the top ten origination points for attached malware thus far in 2021. The most noteworthy shift we observed this year was an 240% increase over 2020 for malware traffic originating from China.



Below is a list of the most common malware attachment file type as observed by our filters throughout 2021. Malicious HTM/HTML attachments were on an upward trend throughout the entire year.



Data Breaches

Colonial Pipeline

In August, the country's largest fuel pipeline learned that threat actors exfiltrated documents containing the personal information of other 5,800 individuals. This data breach resulted from the DarkSide ransomware attack in May that caused shortages across the East coast stemming from a single compromised password.

Colonial Pipeline revealed in its data breach notification that "the affected records contained certain personal information, such as name, contact information, date of birth, government-issued ID (such as Social Security, military ID, tax ID, and driver's license numbers), and health-related information (including health insurance information)."

Kaseya

The software vendor that supports the Managed Service Provider (MSP) market through its VSA tools was the perfect conduit for one of the largest supply chain attacks to date. In early July, REvil ransomware was deployed to MSPs via a fake software update using Kaseya VSA. The REvil ransomware then spread from the MSPs to between 800 and 1,500 businesses worldwide, with many of these MSPs each having thousands of impacted endpoints. The actual figure remains unclear, but the threat actors claimed to have hit 1 million endpoints.

Accenture

The global consulting firm fell victim to a LockBit ransomware attack in August. The LockBit ransomware group demanded a $50 million ransom and claimed to have stolen 6 terabytes of data from Accenture's network. The threat group also claimed they had collected sufficient data to breach some Accenture clients, including Bangkok Airways (200GB of passenger data) and Ethiopian Airlines.

However, there was a lot of pushback against these claims by Accenture, a spokesperson for the company stated "Through our security controls and protocols, we identified irregular activity in one of our environments. We immediately contained the matter and isolated the affected servers." They went on to say, "We fully restored our affected systems from backup, and there was no impact on Accenture's operations, or on our clients' systems."

Twitch

In October, the Amazon-owned live streaming service was subject to a server configuration change which allowed improper access by an unauthorized third party that led to 125GB of data being exflitrated and posted on 4chan. The exposed data primarily consisted of documents from Twitch's source code repository, as well as a subset of creator payout data.

In a statement from Twitch the company stated "Twitch passwords have not been exposed. We are also confident that systems that store Twitch login credentials, which are hashed with bcrypt, were not accessed, nor were full credit card numbers or ACH/bank information."

Acer

The Taiwanese electronics and computer maker was hit by a REvil ransomware attack in March that led to a $50 million ransom demand. Over 60GB of data was exfiltrated which included sensitive customer information such as names, client phone numbers, financial spreadsheets, bank balances, and bank communications. Acer's entire response to the incident is below:

"Acer routinely monitors its IT systems, and most cyber attacks are well defensed. Companies like us are constantly under attack, and we have reported recent abnormal situations observed to the relevant law enforcement and data protection authorities in multiple countries."

"We have been continuously enhancing our cybersecurity infrastructure to protect business continuity and our information integrity. We urge all companies and organizations to adhere to cyber security disciplines and best practices and be vigilant of any network activity abnormalities."

T-Mobile

In August, the mobile telecommunication company was breached by a highly sophisticated cyber attack that affected more than 40 million of their customers. In a statement the telecom giant said "Fortunately, the breach did not expose any customer financial information, credit card information, debit or other payment information but, like so many breaches before, some SSN, name, address, date of birth and driver's license/ID information was compromised."

Volkswagen

In June it was revealed that the German motor vehicle manufacturer was impacted by a data breach affecting over 3.3 million customers. An unauthorized third party accessed this information through an associate vendor which was not identified.

Per their statement: "This included information gathered for sales and marketing purposes from 2014 to 2019. Audi and Volkswagen believe the data was obtained when the vendor left electronic data unsecured at some point between August 2019 and May 2021, when the source of the incident was identified."

Neiman Marcus

The US-based retailer confirmed unauthorized access to customer online accounts in September. Per the company's statement: "The personal information for affected Neiman Marcus customers varied and may have included names and contact information; payment card numbers and expiration dates (without CVV numbers); Neiman Marcus virtual gift card numbers (without PINs); and usernames, passwords, and security questions and answers associated with Neiman Marcus online accounts. Approximately 4.6 million Neiman Marcus online customers are being notified of this issue. For these customers, approximately 3.1 million payment and virtual gift cards were affected, more than 85% of which are expired or invalid. No active Neiman Marcus-branded credit cards were impacted."

ParkMobile

In March, the popular mobile parking app became aware of a cybersecurity incident linked to a vulnerability in a third-party software the company utilizes. This subsequently led to account information for 21 million customers being sold on the dark web. The company stated:

1. The investigation confirmed that no credit card information was accessed.
2. No data related to a user's parking transaction history was accessed.
3. Only basic user information was accessed. This includes license plate numbers, as well as email addresses, phone numbers, and vehicle nicknames, if provided by the user. In a small percentage of cases, mailing addresses were also affected.
4. Encrypted passwords were accessed, but not the encryption keys required to read them. We protect user passwords by encrypting them with advanced hashing and salting technologies.
5. We do not collect Social Security numbers, driver's license numbers, or dates of birth.

Bonobos

In January, the men's clothing store fell victim to a massive data breach which exposed millions of customers' personal information due to a threat actor downloading a cloud backup of their database. The threat actor in question is the notorious ShinyHunters who is well known for hacking online services and selling stolen databases. The leaked database is 70GB in size containing information such as customers' addresses, phone numbers, partial credit card numbers (last 4 digits), password histories, and order information. The company stated they "have found no evidence of unauthorized parties gaining access to Bonobos' internal system" and "Payment information was not affected by this issue."

Kronos

On December 11 the HR management platform was taken down by a ransomware attack. Three days later Kronos' parent company UKG stated "we became aware of unusual activity impacting UKG solutions using Kronos Private Cloud. We took immediate action to investigate and mitigate the issue and have determined that this is a ransomware incident affecting the Kronos Private Cloud—the portion of our business where UKG Workforce Central, UKG TeleStaff, Healthcare Extensions, and Banking Scheduling Solutions are deployed."

UKG went on to say they expected several weeks of downtime due to the attack. This led organizations reliant on the provider to scramble to alternative options to maintain business continuity. In addition to the outage, Kronos has also stated that information of many of its customers may have been stolen in the attack.

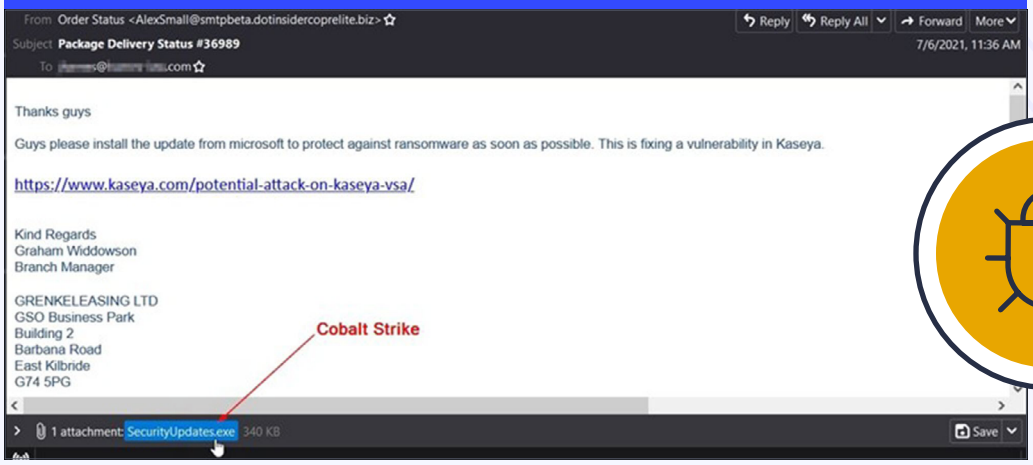
Events Leveraged

Supply Chain Attacks Maximize Compromise

News of the supply chain ransomware distribution attack against enterprise technology firm Kaseya made waves in July. In that event, the REvil ransomware group compromised Kaseya software that is used primarily by MSPs and their customers. The malicious actors were able to push out a fake software update titled "Kaseya VSA Agent Hot-fix", which was the REvil ransomware package. This is said to have affected some 800-1200 Kaseya customers. REvil quickly demanded the sum of $70 million in exchange for a blanket decryption tool. Kaseya was able to obtain (without paying the ransom) a decryption tool which reportedly worked on 100% of the effected files, though some mystery remains around where they obtained the key.

As the story made headlines over a holiday weekend in the US, many IT workers quickly scrambled to make sure they were not affected. Attempting to capitalize on the chaos, malware distributors looked to take advantage and double down. Just a few days after the event, we began capturing a malicious email campaign attempting to pose as a security patch related to Kaseya. The malicious emails instructed the recipient to open an attached executable file to fix the Kaseya vulnerability. This attack theme was quite timely as it preys upon the uncertainty and fear surrounding this high-profile incident. Attackers are always eager to capitalize upon prominent new events which provide better odds of successful exploitation attempts.

EXAMPLE: KASEYA-THEMED MALWARE ATTACK



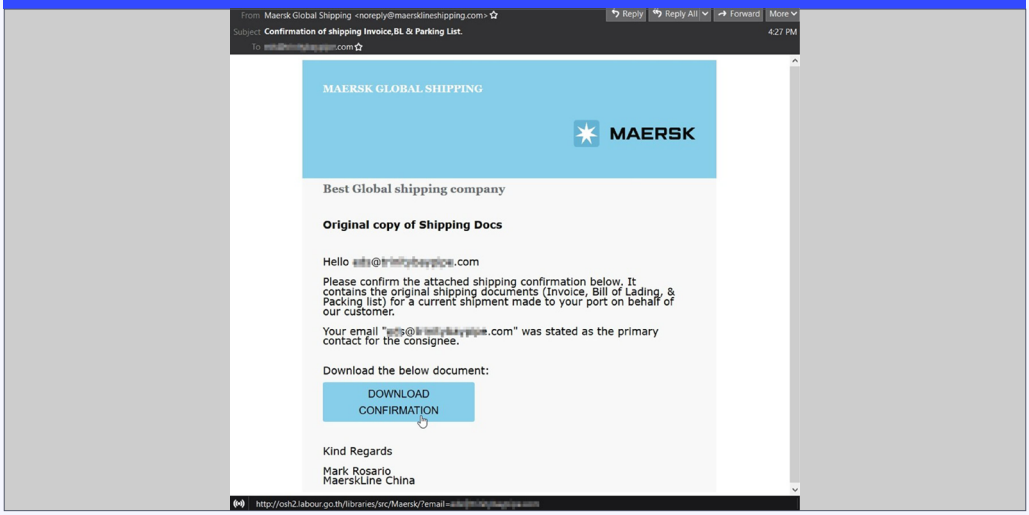
The attached executable file contained Cobalt Strike. This penetration testing tool is commercially available and often used by security researchers and red teams to help discover and mitigate network vulnerabilities. However, the use of the Cobalt Strike tool for malicious exploitation has grown 161% this year as threat actors have been able to obtain cracked versions and backdoor the tool.

[PRO-TIP]: Remember that security advisories and applicable patches for them are a common theme used in malware and phishing attacks. Once a vulnerability is discovered, it's literally a race between threat actors attempting to exploit it and the applicable vendor to issue patches to help prevent compromise.

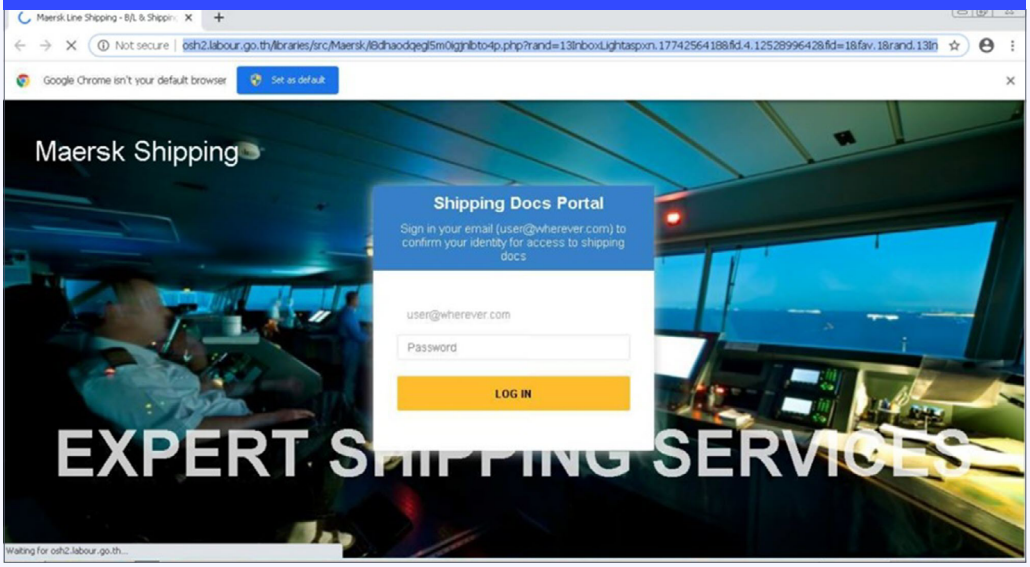
Global Shipping Issues Leveraged

With vast shipping delays and supply chain issues around the world, threat actors were eager to spoof logistics and transportation companies looking for an express lane to compromise victims. Below is an example that we captured posing as Maersk. It urged the user to download shipping confirmations by clicking on a link.

EXAMPLE



If the user complies, they are directed a phishing site located on labour.go[.]th. The page cycles through different realistic-looking Maersk backgrounds with a sign-in screen overlayed to steal the users' email credentials. Per whois DNS data, the domain itself appears to be a Thai government page managed by the Labor Protection and Welfare Department. This wasn't the only attack we captured sent from or hosted on government sites from around the world, although it is a prime example that shows everyone is considered fair game to threat actors.

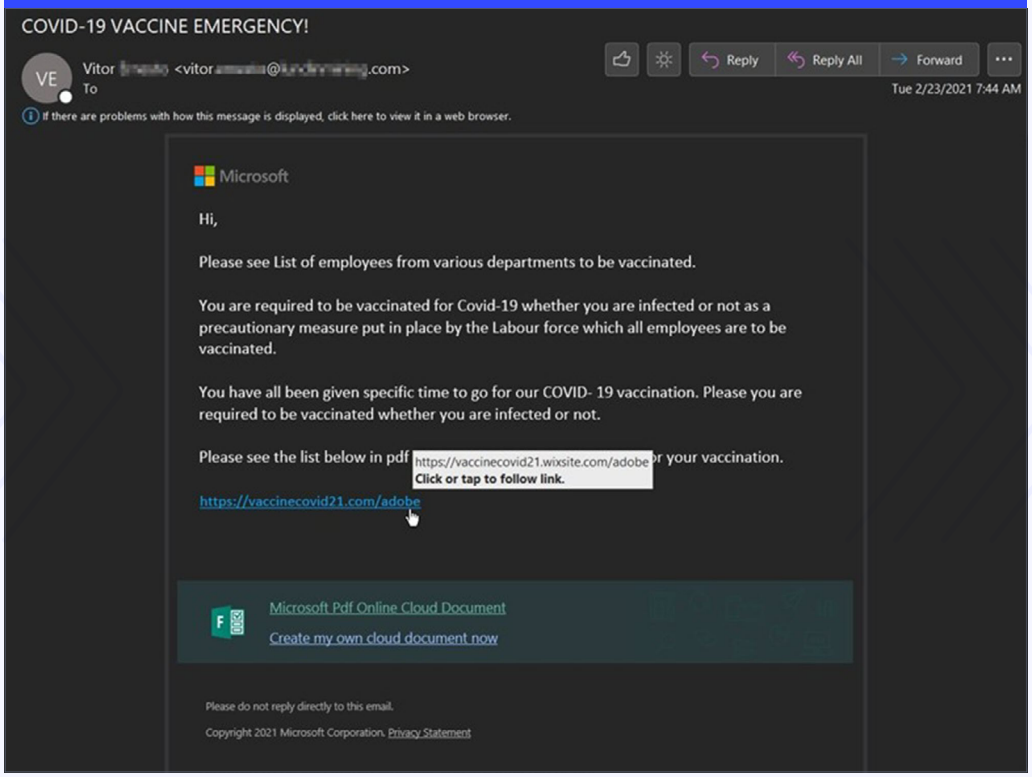


COVID-19/Omicron

Attackers continued to leverage the pandemic theme to distribute both phishing and malware attacks. It's no surprise that throughout the year we continued to see this topic used for social engineering attacks.

One of the COVID-19 themed LotL attacks we captured stated, "a team member has been infected with Covid-19" and to see the below names of suspected cases and stay isolated from them. Another from the same actor, pictured below, stated to "see list of employees from various departments to be vaccinated." Both messages contained a payload link to a "Microsoft PDF Online Cloud Document." The actor utilized phishing links to both the Weebly and Wix websites and form builders to conduct these Living Off the Land attacks, however, both links led to an Adobe PDF Online Cloud Document themed phishing page designed to steal user credentials.

EXAMPLE 1



It didn't take long for threat actors to attempt to leverage uncertainty surrounding the Omicron (COVID-19) variant to help distribute their payloads. The attack below was spotted in late November and contained the GULoader trojan downloader. GULoader has been used since December of 2019 to load mainly info-stealers and RATs such as Formbook, Agent Tesla and Netwire.

EXAMPLE 2

Re:RE: Proforma Invoice\\NEW GOVERNMENT POLICY// Awaiting Vessel Departure confirmation\\ EXW-4098...

Reply | Reply All | Forward

SY Stevie [redacted] <stevie.[redacted]@[redacted].com>
To [redacted]@[redacted].com

Tue 11/30/2021 9:32 PM

P-INV DEC-21 PO-409865-00454357527018_pdf.arj
69 KB

Dear valued customer,

Please find attached PI. Still pending for confirmation of vessel.

Kindly note that Government has some new policy in response to the OMICRON COVID-19 strain outbreak.

Documents will be sent following final confirmation.

Best Regards

Stevie Yuanita (Export section)
PT Tunas Alfin Tbk
Imperium Tower 28th Floor, Metropolitan Kuningan Superblock
Jl. HR Rasuna Said Kav. No. 1
Jakarta 12980
Phone : 021-8317322
Fax : 021-8317683

2022 Predictions

Manufactures Beware: Sector Will Experience Double-Digit Increase in Cyberattacks

Manufacturing is already a rich target for those seeking to carry out attacks on critical infrastructure. As supply chain issues continue into 2022, this period of disruption will provide ample opportunities for attackers, who thrive in times of increased uncertainty. This will make the manufacturing and distribution industry one of the most targeted industries for cybercriminals next year.

Personalized Phishing Will Require More Defense Specificity

Spear-phishing attacks, which involve cybercriminals personalizing emails to fit a smaller group of individuals than traditional tactics and appear more authentic, are not going anywhere. As the rise in personalized phishing gives way to new customization tactics in 2022, organizations and defenders will respond by prioritizing building more specificity into their email defenses.

SMBs Must Be Prepared for Ransomware-as-a-Service Proliferation

In 2022, the Ransomware-as-a-Service model will see continued growth as it has proven to be an incredibly efficient vehicle for maximizing profits. Government involvement in defense of critical infrastructure will motivate ransomware groups to target softer targets, such as small and medium-sized businesses (SMBs), to draw less attention and news than larger, high-profile targets.

Cybersecurity Insurance will become a Necessity for SMB Survival

Cybersecurity insurance was once only utilized by larger companies that were considered the highest-value targets. The proliferation of Malware-as-a-Service (MaaS) and Ransomware-as-a-Service (RaaS) offerings on the dark web and underground forums has drastically changed the threat landscape. More SMBs will realize (hopefully not the hard way) they are also a target for ransomware, extortion, and data theft attacks. The insurance industry offerings will evolve to ensure that businesses can protect themselves, with the personalized coverage needed, in the unfortunate event of an incident.

There Will Be Greater Coordination and Collusion Between Threat Groups

As we have seen with the evolution of Malware-as-a-Service and Phishing-as-a-Service, threat actors are willing to join forces for mutual success. This was further demonstrated in the aftermath of the Emotet cybercrime services takedown earlier this year. After Emotet services were disabled by law enforcement, Trickbot malware operators stepped in and began re-seeding Emotet infections to get them back into operation. As a result, we saw malicious email traffic from Emotet on November 15th for the first time since the takedown in January 2021. Even threat actors competing for profits see the value in having a greater variety of threat actors in operation. They can leverage them as a service or even hide their activities better in the noise. That is why in 2022, we will see cybercriminals form even more robust working relationships to facilitate their continued success.

Supply Chain Attacks

The Kaseya and SolarWinds attacks highlighted how efficient and effective attack efforts can be when an attacker is able to breach a trusted link in the supply chain. The fallout from this type of compromise can trickle down to everyone else that utilizes the product or service. We anticipate threat actors will increasingly devote more time and resources to attack supply chains to multiply the number of compromised victims.

Companies Increasingly Adopt Cloud Migrations and Virtualization in move closer to Zero Trust

The growth of the remote work force has further necessitated the need to migrate company resources (software, data, and physical) to cloud-based technologies. With services such as Microsoft's Windows 365 Cloud PC rolling out this year, we believe that the easily scalable virtualized PC environment will take market share from traditional expensive physical machines and the need for IT staff to maintain them.

Email Bombs Will Increase in Occurrence and Severity

Email bombs are a type of email-based Denial of Service (DoS) and vary in severity from anywhere between 1,000 to over 200,000 messages over a very short period. Attackers do this by subscribing to thousands of legitimate newsletters and website forms that do not require a form of live-user verification. Targets receive an uncontrollable flood of emails that are a distraction for fraudulent purchases or financial account updates or transactions. We have observed multiple cases now where more than one employee in the same organization is targeted simultaneously.

As an unwanted side-effect, aggressive email bombs may effectively burn the email address since the victim will endlessly receive newsletter traffic. We have found the victims' address might also be shared with cybercriminal groups for follow-up phishing and malware attacks. In May of 2017 we were able to convince an unsuspecting email bomber on the dark web to bomb a test address on a domain under our control with 50,000 messages. This address was used for nothing else; it still receives 30-70 unwanted emails a day—90% are newsletters or spam, 7% malware and 3% phishing.