



Advanced Security Operations Center
Telelink Business Services
www.telelink.com

Monthly Security Bulletin

December 2020

This security bulletin is powered by Telelink's Advanced Security Operations Center

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and predictable monthly fee.



Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor's solutions.
- Can be sized to fit small, medium and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

LITE Plan

425 EUR/mo

- Gain visibility on the security posture of all your company's IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company's security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis and cyber threat mitigation!

Table of Contents

1.	Scammers Abuse Google Drive to Send Malicious Links.....	4
2.	34M Records from 17 Companies Up for Sale in Cybercrime Forum.....	5
3.	New Pay2Key ransomware encrypts networks within one hour	7
4.	Helping Your Family Combat Digital Misinformation	10
5.	Fake Microsoft Teams updates lead to Cobalt Strike deployment	12
6.	Ransomware Group Turns to Facebook Ads.....	14
7.	How AI Can Make Cybersecurity Jobs Less Stressful and More Fulfilling	16
8.	Be Very Sparing in Allowing Site Notifications.....	20
9.	Google’s free services are now phishing campaign’s best friends	25
10.	IBM CISO Perspective: Zero Trust Changes Security From Something You Do to Something You Have.....	29
11.	Passwords exposed for almost 50,000 vulnerable Fortinet VPNs	31
12.	Sophos alerts customers of info exposure after security breach	34
13.	The Future of Cybersecurity: How to Prepare for a Crisis in 2020 and Beyond...	36

1. Scammers Abuse Google Drive to Send Malicious Links

Scammers are leveraging a legitimate Google Drive collaboration feature to trick users into clicking on malicious links.

According to reports,, the recent attack stems from Google Drive's legitimate collaboration feature, which allows users to create push notifications or emails that invite people to share a Google doc. Attackers are abusing this feature to send mobile users Google Drive notifications that invite them to collaborate on documents, which then contain malicious links.

Because they are sent via Google Drive, the notifications come from Google's no-reply email address, making them appear more legitimate. Other iterations of the attack are sent via email (instead of by notification) and include the malicious link right in the email.

"Interesting TTP utilising Google Sheets, ultimately ending up with generic prize scams," said a cybersecurity expert who goes by Jake (or @JCyberSec) on Twitter. "Google sheets slide was shared with an email address causing a pop-up notification on mobile."

The attack is targeting hundreds of thousands of Google users, according to WIRED. The report said that the notifications are being sent in Russian or broken English.

The Google Drive notifications come with various lures. Many purport to be "personal notifications" from Google Drive, with one lure entitled "Personal Notification No 8482" telling the victim they haven't signed into their account in awhile. These threaten that the account will be deleted in 24 hours unless they sign in via a (malicious) link. Another, entitled "Personal Notification No 0684," tells users they have an "important notice" of a financial transaction that they can view on their personal account, via a link.

One purports to be a run-of-the-mill prize scam that pretends to be part of a "Chrome Search contest 2020" and tells victims that they are the 5-billionth search and have won a prize.

These links take victims to malicious scam websites. WIRED reported that one such website flooded users with notifications to click on links for "prize draws," while other websites requested that victims click on links to "check their bank account."

Targeted users took to Twitter to warn of the scams, with one Twitter user saying that the only red flag of the scam was that he wasn't expecting a shared doc.

A Google spokesperson told WIRED that the company is working on new security measures for detecting Google Drive spam. Threatpost has reached out to Google for further comment.

With the prevalence of working from home due to the coronavirus pandemic, attackers are increasingly leveraging collaboration and remote-work tools, including Google offerings. In May, researchers warned of a series of phishing campaigns using Google Firebase storage URLs. These used the reputation of Google's cloud infrastructure to dupe victims and skate by secure email gateways. Meanwhile, researchers in October warned of a phishing campaign that pretends to be an automated message from Microsoft Teams. In reality, the attack stole Office 365 recipients' login credentials.

"This scam wave highlights the need for users to be on the lookout for email-borne attacks," according to Tripwire researchers. "Organizations can help their users in this regard by educating them about some of the most common types of phishing attacks that are in circulation today.

Source: <https://threatpost.com/scammers-google-drive-malicious-links/160832/>

2. 34M Records from 17 Companies Up for Sale in Cybercrime Forum

A diverse set of companies, including an adaptive-learning platform in Brazil, an online grocery service in Singapore and a cold-brew coffee-maker company, are caught up in the large data trove.

A whopping 34 million user records have materialized on an underground sales forum, which cybercriminals claim are gleaned from 17 different corporate data breaches.

According to reports, the data appeared late last week, and the theft appears to be the work of a single person or group.

The affected companies are a widely diverse set of targets, gleaned from around the world. According to Bleeping Computer, they include: Apps-builder.com; Athletico in Brazil; Indonesian financial firm Cermati; Clip (a card-reader company in Mexico); Coupontools.com; Eatigo; Everything5pounds.com; Fantasy Cruncher (a fantasy sports tool); Game24h in Vietnam; Geekie; online video-maker Invideo; lease-to-own furniture company Katapult; RedMart; Toddycafe (which offers cold-brew coffee gear); W3layouts (website templates); Indian wedding planning service Wedmegood; and Wongnai.

Two of the breaches were previously reported: RedMart and Eatigo.

RedMart (a division of Lazada, owned by Chinese giant Alibaba), offers online grocery shopping and delivery in Singapore. It's perhaps the highest-profile company on the list – the company confirmed the incident in a notice to customers.

A full 1.1 million records were stolen from the company and put up for sale, containing emails, SHA1 hashed passwords, mailing and billing addresses, full names, phone numbers, partial credit-card numbers and expiry dates. The price tag for the cache is \$1,500, according to the Straits Times, a Singapore-area paper of record.

"Our cybersecurity team discovered an individual claiming to be in possession of a RedMart customer database taken from a legacy RedMart system no longer in use by the company," according to the company's statement. "This RedMart-only information is more than 18 months out of date and not linked to any Lazada database...current customer data" is not affected.

Meanwhile Eatigo, which offers online restaurant reservations in Singapore and neighboring areas, said that data from 2.8 million accounts was stolen and offered for sale. In an email to affected customers, also reported by the Straits Times, the company said the data was more than 18 months old.

"We were made aware on Oct 30th that along with several other e-commerce platforms, we were the subject of a data security incident," the company said. "Your existing Eatigo account password is protected by encryption and hence safe. We do not store credit-card information on our system."

The affected data includes emails, passwords, names, phone numbers, gender, and Facebook IDs and tokens.

The other company to confirm a breach is Wongnai, Thailand's equivalent to Yelp. That database included 4.3 million records, the attacker said, containing emails, passwords, Facebook and Twitter IDs, names, birthdates, phone numbers and postal codes. It confirmed the breach via email, according to Bleeping Computer.

"Thanks for your inquiry, we were aware of this incident last night (Bangkok time) and our tech team have been investigating this matter," the company told the outlet.

Another breach of note in the trove is the compromise of Geekie, which is an adaptive-learning platform sanctioned by the Brazilian government and used by 5,000 different schools there. It reportedly had the most records put up for sale: A full 8.1 million of them are on offer, containing emails, bcrypt-sha256/sha512 hashed passwords, usernames,

names, dates of birth, gender, mobile phone numbers and Brazilian CPF numbers (taxpayer IDs).

Meanwhile, the seller of the data on the underground forum told Bleeping Computer that he was merely a broker, acting on behalf of the actual attacker.

"When asked how the hacker gained access to the various sites, the seller stated, 'Not sure if he want to disclose,'" according to the report.

Massive Credential Dumps

This latest incident continues the sporadic trend of massive data dumps showing up online (which generally lead to follow-on phishing and account take-over efforts).

In January, a huge cache totaling 87 GB of data was spotted on the MEGA cloud service. The data was organized into 12,000 separate files under a root folder called "Collection #1." But as it turns out, Collection #1 was only a fraction of a larger amount of leaked credentials.

Soon after, researchers at the Hasso Plattner Institute in Potsdam, Germany discovered another new trove of stolen data equaling 845 GB and 25 billion records in all (611 million credentials after de-duping). The latest data dump, dubbed "#Collection #2-5" contained roughly three times as many unique records as Collection #1.

In all, the entire set of compromised credentials totaled 993.53 GB of data, including addresses, cell phone numbers and passwords.

Source: <https://threatpost.com/34m-records-17-companies-cybercrime-forum/160923/>

3. New Pay2Key ransomware encrypts networks within one hour

A new ransomware called Pay2Key has been targeting organizations from Israel and Brazil, encrypting their networks within an hour in targeted attacks still under investigation.

Michael Gillespie, the creator of ID Ransomware, has also seen submissions from Pay2Key victims predominantly from Brazilian IP addresses.

Although used in attacks against multiple Brazilian entities, this ransomware is not related to yesterday's RansomExx attacks targeting Brazil's government networks.

Encrypts networks within one hour

In a new report by Check Point, researchers say that the threat actors behind Pay2Key ransomware are likely using publicly exposed Remote Desktop Protocol (RDP) to gain access to victims' networks and deploy the initial malicious payloads.

While the Pay2Key operators infiltrate and are active in the targeted networks before the ransomware begins encrypting systems, they have the "ability to make a rapid move of spreading the ransomware within an hour to the entire network."

Once inside a victim's network, the attackers will set up a pivot device that will be used as a proxy for all outgoing communications between the ransomware infected computers and Pay2Key's command-and-control (C2) servers.

This helps them evade or at least reduce the risk of detection before encrypting all reachable systems on the network by using a single device to communicate with their own infrastructure.

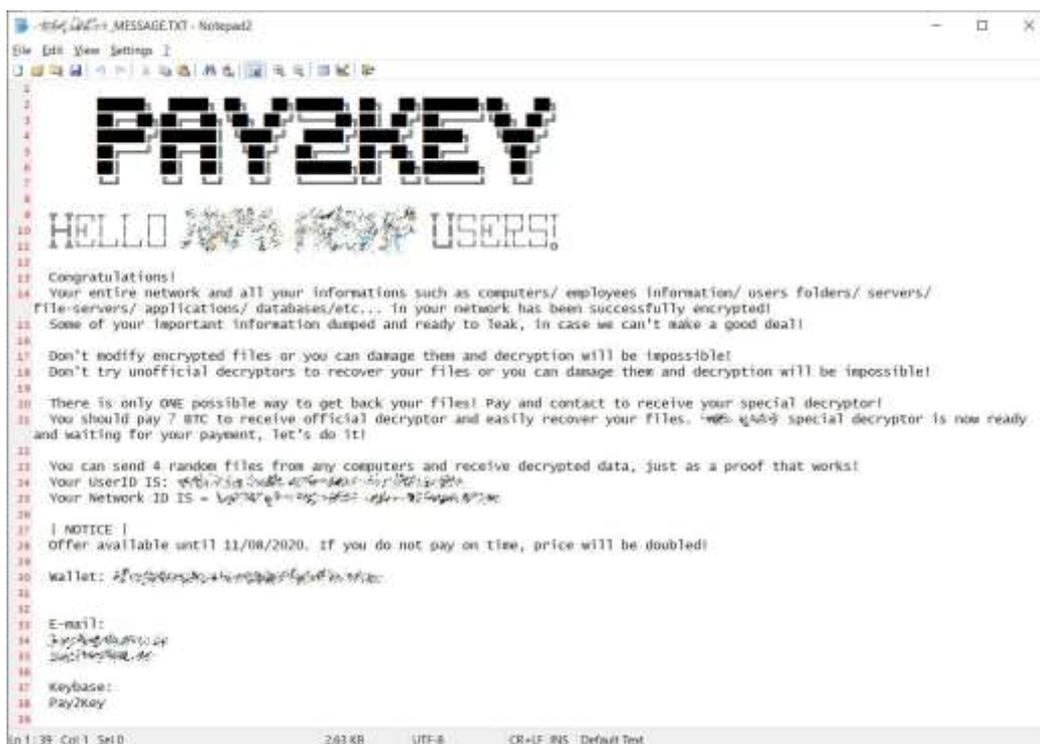
Ransoms up to \$140K

Just as in the case of other human-operated ransomware operations, Pay2Key actors will use Microsoft's legitimate PsExec portable tool to remotely execute ransomware payloads named Cobalt.Client.exe on the targeted organizations' network devices.

Following successful encryption of a device, the ransomware will drop a ransom note on the system, customized for each compromised organization, and using a [ORGANIZATION]_MESSAGE.TXT name.

The ransom note also mentions that some of the victims' files was stolen during the attacks but Check Point is yet to find proof of this happening.

Pay2Key operators are currently asking for relatively low ransoms, with Check Point seeing them demand between 7 and 9 bitcoins (roughly \$110K-\$140K) per victim. BleepingComputer has seen ransom demands as low as 4 bitcoins (around \$62K).



```

1
2
3
4
5
6
7
8
9
10 HELLO 用户!
11
12 Congratulations!
13 Your entire network and all your informations such as computers/ employees information/ users folders/ servers/
14 file-servers/ applications/ databases/etc... in your network has been successfully encrypted!
15 Some of your important information dumped and ready to leak, in case we can't make a good deal!
16
17 Don't modify encrypted files or you can damage them and decryption will be impossible!
18 Don't try unofficial decryptors to recover your files or you can damage them and decryption will be impossible!
19
20 There is only ONE possible way to get back your files! Pay and contact to receive your special decryptor!
21 You should pay 7 BTC to receive official decryptor and easily recover your files. 我们有一个特殊的解密器现在准备好了
22 正在等待您的付款, 让我们做它!
23
24 You can send 4 random files from any computers and receive decrypted data, just as a proof that works!
25 Your UserID IS: 00000000000000000000000000000000
26 Your Network ID IS = 00000000000000000000000000000000
27
28 | NOTICE |
29 offer available until 11/08/2020. if you do not pay on time, price will be doubled!
30
31 wallet: 00000000000000000000000000000000
32
33
34 E-mail:
35 00000000000000000000000000000000
36 00000000000000000000000000000000
37
38 keybase:
39 Pay2Key
40
Ln 1: 33 Col 1: Set 0 249 KB UTF-8 CR+LF INS Default Text

```

Pay2Key ransom note

This ransomware is not based on code from previously detected strains and Pay2Key samples were only detected by a single antimalware engine when submitted to VirusTotal.

According to compilation artifacts, it also looks like Pay2Key is internally called 'Cobalt' by developers who are not native English speakers according to strings and log wording.

The ransomware uses a hybrid of symmetric and asymmetric encryption scheme which employs the AES and RSA algorithms with the C2 server being the one to deliver an RSA public key at runtime which indicates that Pay2Key will fail to encrypt machines without an Internet connection or if the C2 server is offline.

"While the attack is still under investigation, the recent Pay2Key ransomware attacks indicate a new threat actor is joining the trend of targeted ransomware attacks – presenting well-designed operation to maximize damage and minimize exposure," the Check Point researchers concluded.

Source: <https://www.bleepingcomputer.com/news/security/new-pay2key-ransomware-encrypts-networks-within-one-hour/>

4. Helping Your Family Combat Digital Misinformation

If 2020 has taught us anything, it's that our ability to think critically about the information we encounter online is now a fundamental life skill we need to learn, practice, and pass on to our offspring. But the actual task of teaching kids how to discern real and fabricated information online these days is easier said than done.

How did the truth get so hard to pin down? In the documentary *The Social Dilemma*, the answer to that question comes down to two things: Our growing reliance on social media for both human connection and information and the data-based algorithms social networks use to mine and sell data, nurture device dependence, and influence our behavior.

A [2019 Pew Study](#) reveals that 55 percent of US adults get their news from social media either "often" or "sometimes." A [July 2020 Pew Study](#) shows that people who rely on social media for news are less likely to get the facts right about the coronavirus and politics and more likely to hear some unproven claims.

The power of algorithms to deliver customized, manipulative content to a person's screen is alarming, says Tristan Harris, a former design ethicist at Google, who is featured in *The Social Dilemma*, adding, "Never before in history have 50 designers made decisions that would have an impact on two billion people."

Fighting Back

On the heels of the recent election, Media Literacy skills will make a difference as [false reports are likely to surface in our social feeds](#) in the foreseeable future. For many, the willpower to shut down their social feeds altogether isn't a viable option. So how do we wade through the veiled forms of manipulation and misinformation taking place all around us online?

One approach is to make a personal commitment to stay alert, slow down, and carefully vet the content you consume, create, or share.

Media Literacy

One thing you might consider is making 2021 the year your family masters Media Literacy, a topic we've [written extensively about on this blog](#). In short, Media Literacy is the ability to identify different types of content and understand the messages each is sending. Content includes texts, social media memes or posts, videos, television, movies, video games, music, and various other digital content. Reminder: Someone creates each piece of content and that person, group, or company has an agenda or message.

Grow Your Family's Media Literacy Muscle

- **Watch:** *The Social Dilemma* is a must-see for families. The Netflix film blends documentary investigation and narrative drama to explain the hidden maneuvers behind social media and search platforms. Watch it. Talk about it. Do social media wiser in 2021.
- **Go Deeper:** *The Social Dilemma* refers to books written by the people interviewed and includes collateral video clips. *Medium* put together this [great list of supporting quotes and resources](#) from the film.
- **Read:** Stories are powerful ways to teach kids of any age how to process the digital world around them. The Media Literacy thought leaders at [Cyberwise recently created this list of children's books](#) designed to teach kids how to think critically and become informed consumers of online media.
- **Fact-check.** Even kids have a responsibility to share truthful content online. Discuss how to fact check articles and rumors before sharing. Here are a few resources:
 - [PolitiFact](#) from the Poynter Institute
 - [AP News Fact Check](#) from the Associated Press
 - [Reuters Fact Check](#) from Reuters News
- **Discuss:** Talk about the practical ways of challenging each piece of content by asking:

Do I understand all the points of view of this story?

What do I think about this topic or idea?

Am I overly emotional and eager to share this?

Am I being manipulated by this content?

What if I'm wrong?

Lastly, consume all media with thoughtful intention — avoid mindless scrolling and liking. A few other practical ways to fight back against the algorithms we drew from *The Social Dilemma*: Don't click on video or content recommendations. Fight back against algorithms by choosing your content. Uninstall social media apps that are not useful and waste your time. Turn off notifications or any other alert that interferes with living life. If an issue has you angry or emotional, stop, breathe, and research the facts before sharing.

The post [Helping Your Family Combat Digital Misinformation](#) appeared first on [McAfee Blogs](#).

Source: <https://www.mcafee.com/blogs/consumer/family-safety/combat-digital-misinformation/>

5. Fake Microsoft Teams updates lead to Cobalt Strike deployment

Ransomware operators are using malicious fake ads for Microsoft Teams updates to infect systems with backdoors that deployed Cobalt Strike to compromise the rest of the network.

The attacks target organizations in various industries, but recent ones focused on the education sector (K-12), which depends on videoconferencing solutions due to Covid-19 restrictions.

From infostealer to Cobalt Strike

In a non-public security advisory seen by BleepingComputer, Microsoft is warning its customers about these FakeUpdates campaigns, offering recommendations that would lower the impact of the attack via its Defender ATP service.

FakeUpdates attacks were seen in 2019 delivering DoppelPaymer ransomware. But this year, the malvertising campaigns dropped WastedLocker and showed technical evolution.

For instance, they started using signed binaries and various second-stage payloads.

More recently, the attackers exploited the [ZeroLogon](#) (CVE-2020-1472) critical vulnerability to gain admin access to the network. This occurred via the SocGhosh JavaScript framework, found earlier this year on [dozens of hacked newspaper sites](#) owned by the same company.

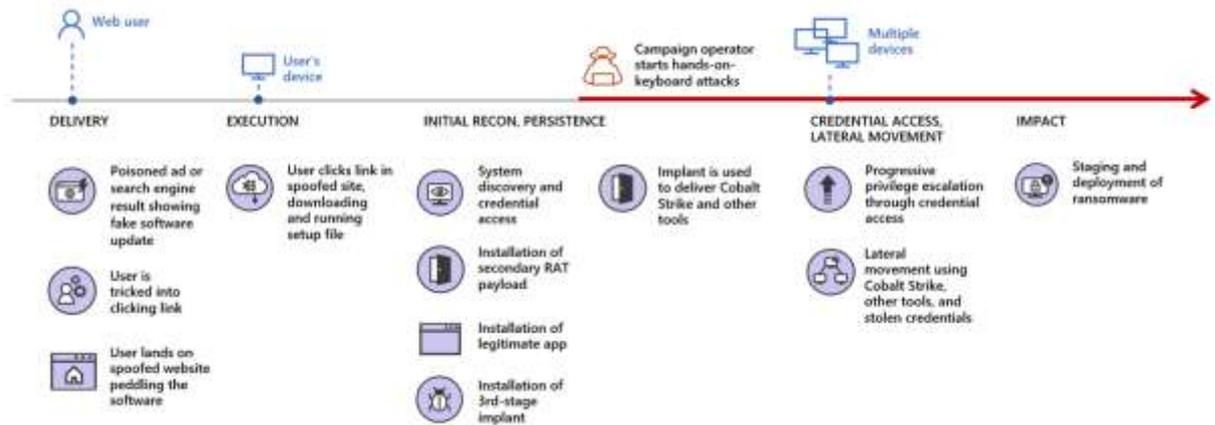
Planting the malicious fake ads that lure unsuspecting users into clicking it to install an update was possible by poisoning search engine results or through malicious online advertisements.

In at least one attack Microsoft detected, the crooks purchased a search engine ad that caused top results for Teams software to point to a domain under their control.

Clicking on the link downloaded a payload that executed a PowerShell script to retrieve more malicious content. It also installed a legitimate copy of Microsoft Teams on the system to keep victims unaware of the attack.

Microsoft says that in many cases the initial payload was Predator the Thief infostealer, which sends the attacker sensitive information like credentials, browser, and payment data. Other malware distributed this way includes Bladabindi (NJRat) backdoor, and ZLoader stealer.

The malware also downloaded other payloads, with Cobalt Strike beacons being among them, thus allowing the attacker to discover how they could move laterally across the network.



In several of the observed attacks, the last stage was detonating file-encrypting malware on the network computers.

Microsoft is warning that the same patterns seen in the FakeUpdates campaigns using Teams updates as lure were observed in at least six others, suggesting the same actor behind them. In some variations of the same theme, the attacker used the IP Logger URL shortening service.

Mitigation advice

Microsoft recommends using web browsers that can filter and block malicious websites (scam, phishing, malware and exploit hosts) along with using strong, random passwords for local administrators.

Limiting admin privileges to essential users and avoiding domain-wide service accounts that have the same permissions as an administrator are also on the list of measures that would reduce the impact of an attack.

To minimize the attack surface, Microsoft recommends blocking executable files that do not meet specific criteria such as prevalence and age or are outside a regularly maintained trusted list.

Blocking JavaScript and VBScript code from downloading executable content also adds to the defenses of the environment.

Source: <https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/>

6. Ransomware Group Turns to Facebook Ads

It's bad enough that many ransomware gangs now have blogs where they publish data stolen from companies that refuse to make an extortion payment. Now, one crime group has started using hacked **Facebook** accounts to run ads publicly pressuring their ransomware victims into paying up.



Why You're Seeing This Ad

You're seeing this ad because your information matches **Hodson Event Entertainment's** advertising requests. There

On the evening of Monday, Nov. 9, an ad campaign apparently taken out by the [Ragnar Locker Team](#) began appearing on Facebook. The ad was designed to turn the screws to the Italian beverage vendor **Campari Group**, which [acknowledged on Nov. 3](#) that its computer systems had been [sidelined by a malware attack](#).

On Nov. 6, Campari issued a follow-up statement saying "at this stage, we cannot completely exclude that some personal and business data has been taken."

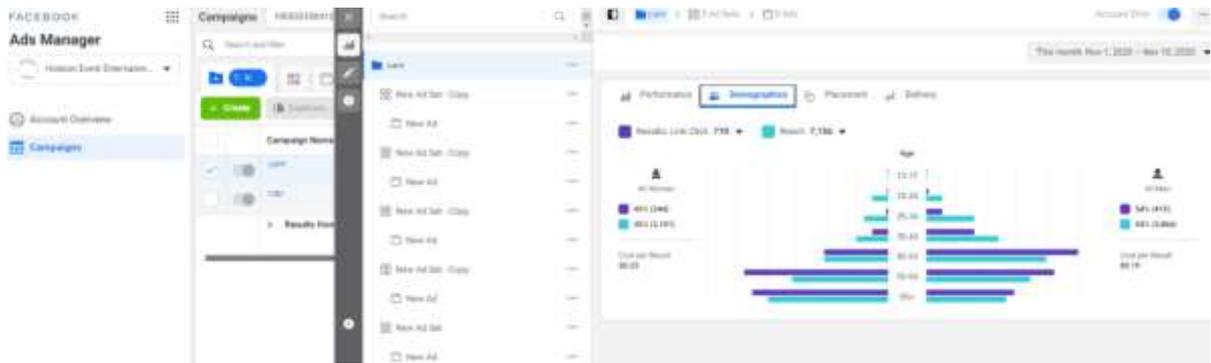
"This is ridiculous and looks like a big fat lie," reads the Facebook ad campaign from the Ragnar crime group. "We can confirm that confidential data was stolen and we talking about huge volume of data."

The ad went on to say Ragnar Locker Team had offloaded two terabytes of information and would give the Italian firm until 6 p.m. EST today (Nov. 10) to negotiate an extortion payment in exchange for a promise not to publish the stolen files.

The Facebook ad blitz was paid for by **Hodson Event Entertainment**, an account tied to [Chris Hodson](#), a deejay based in Chicago. Contacted by KrebsOnSecurity, Hodson said his Facebook account indeed was hacked, and that the attackers had budgeted \$500 for the entire campaign.

"I thought I had two-step verification turned on for all my accounts, but now it looks like the only one I didn't have it set for was Facebook," Hodson said.

Hodson said a review of his account shows the unauthorized campaign reached approximately 7,150 Facebook users, and generated 770 clicks, with a cost-per-result of 21 cents. Of course, it didn't cost the ransomware group anything. Hodson said Facebook billed him \$35 for the first part of the campaign, but apparently detected the ads as fraudulent sometime this morning before his account could be billed another \$159 for the campaign.



The results of the unauthorized Facebook ad campaign. Image: Chris Hodson.

It's not clear whether this was an isolated incident, or whether the fraudsters also ran ads using other hacked Facebook accounts. A spokesperson for Facebook said the company is still investigating the incident. A request for comment sent via email to Campari's media relations team was returned as undeliverable.

But it seems likely we will continue to see more of this and other mainstream advertising efforts by ransomware groups going forward, even if victims really [have no expectation that paying an extortion demand will result in criminals actually deleting or not otherwise using stolen data.](#)

Fabian Wosar, chief technology officer at computer security firm [Emsisoft](#), said some ransomware groups have become especially aggressive of late in pressuring their victims to pay up.

"They have also started to call victims," Wosar said. "They're outsourcing to Indian call centers, who call victims asking when they are going to pay or have their data leaked."

Source: <https://krebsonsecurity.com/2020/11/ransomware-group-turns-to-facebook-ads/>

7. How AI Can Make Cybersecurity Jobs Less Stressful and More Fulfilling

Words for health and the human body often make their way into the language we use to describe IT. Computers get viruses; companies manage their [security hygiene](#); incident response teams train on their [cyber fitness](#). Framing IT concepts in terms of health can also be useful when looking at security operations centers (SOCs) and jobs in cybersecurity.

For many businesses and other entities today, SOCs are not the healthiest they could be. Jobs in cybersecurity can be stressful and overwhelming due to the volume of alerts. Many teams lack the staff they need to keep up with the influx.

The average SOC receives over 11,000 alerts a day, and [28% of all alerts](#) are never addressed, says the 2020 State of Security Operations study from Forrester Consulting, sponsored by Palo Alto Networks.

What would healthier jobs in cybersecurity look like? Imagine fewer alerts organized by priority, and analysts being less stressed as a result. With their time freed up from processing false positives and low-value alerts, analysts could have a chance to dig into higher-value work and advance their careers. Applying AI and machine learning (ML) from detection all the way to response can set SOCs on the path toward achieving this vision for their analysts — and strengthening the group's security postures.

Learn more about AI for cybersecurity

How AI/ML Advances the Health of Your SOC

From sorting alerts to enabling threat sharing, AI/ML can make the SOC more efficient in triage, analysis and response. Connecting the worlds of IT and health care once more, imagine the human body as a stand-in for your IT landscape. Using AI/ML is akin to suggesting the right medical care.

Detecting Issues

First, let's consider detection of known threats. Say someone starts feeling sick with a runny nose and itchy eyes. These symptoms are well-known to them as an allergy flare-up. In some cases, this person skips the doctor's office and heads right to the pharmacy. In others, this person may visit a doctor, who sees these seasonal symptoms, does not see a need for further tests and writes a prescription for the pharmacy.

These familiar symptoms are like a known risk. There are over-the-counter options for allergy relief — in the IT world, these are patches. Adding automation in this scenario is like dropping the right allergy pills on the patient's doorstep, saving a trip to the

pharmacy. AI/ML could detect known risks, spot a signature and update a patch without needing much effort from a human.

Responding Quickly

Jobs in cybersecurity always involve some surprises. What about protecting the body against uncommon illnesses — or threats? Maybe the patient in the first example starts having symptoms that are novel or more severe. The patient visits a medical center, where a nurse takes vitals and a doctor reviews symptoms. Sometimes the doctor asks for more bloodwork or X-rays to get a deeper look at the patient's case. After support staff gathers all the data, the doctor starts forming a diagnosis and treatment. Sometimes, the doctor may ask for more specialists' support.

In the IT metaphor, AI/ML-assisted threat disposition would be like helping the doctor through assistants and labs. AI/ML can help at an early stage by collating data about the IT landscape, as well as from other environments. This speeds up the time to a cure before the illness becomes dire. AI/ML can learn from the analysts' decision making and assist with alert disposition.

Back in the doctor's office, the patient could be having severe discomfort or dysfunction, with parts of the body weakening. Then, the patient needs to be rushed to the hospital. In IT, a team would call for emergency response when IT systems are off-kilter or there is a potential breach. Protecting the IT asset needs to be done right away, and this could involve calling in other specialists for support. By curating everything known about the IT asset, AI/ML could assist the incident response team with forensic analysis and access to playbooks.

Making Jobs in Cybersecurity Less Overwhelming

When AI/ML filters out the flood of low-value alerts through prioritization, analysts spend less time in triage and focus on high-value alerts. Phases of alert prioritization include auto-closure, auto-association and auto-escalation with explainability.

Auto-closure is the machine resolving an alert before it makes its way to the analyst's screen. In terms of our metaphor, it's like seeing another patient with a runny nose and itchy eyes, gathering the enough data about the problem, and prescribing allergy pills without taking up the time of a health care professional.

But, say we have another patient who presents similar symptoms to the person who was supported at the medical center. Then, the doctor can use context, connecting the background on the patient and the symptoms presented. Having more data helps the doctor to prescribe treatment, which will lead to an effective and efficient plan for care. It will also make it easier for the doctor to explain to the patient what's going on.

Auto-escalation with explainability would bring that high-priority case forward with specific details for attention right away. The role of AI/ML here is to make sure the hospital patient is attended to faster, diagnosed for symptoms, and prescribed medication or further treatment urgently. AI supports analysts so specialists can spend their time where it is most needed and resolve critical issues.

A Healthier SOC Leads to Better Jobs in Cybersecurity

When you add up all these ways AI/ML can advance the 'health' of a SOC, the end result is more time. Automation isn't the end goal of applying AI/ML. It's about providing better jobs in cybersecurity to the people hard at work defending these systems.

For example, a Level 1 analyst's day-to-day job might not look all that different as a result of AI/ML. Their work would still involve assessing alerts and conducting research. However, with a machine taking care of the low-value alerts, that analyst would be able to spend more time on fewer cases, going deeper into them. More time could be spent on [breach simulations](#) and tabletop tests that shift the entire team's knowledge and posture from reactive to proactive.

AI/ML could also open brand new avenues for career progression. More time spent researching or focusing on high-value work could help analysts develop skills needed to move to the next level. Or, they might be able to use that time retraining for other critical jobs in cybersecurity like penetration testing, blue squad leadership, analytics, architecture or even an expanded AI/ML role.

Freeing the SOC

At the end of the day, jobs in cybersecurity are just like any other type of work. We want to feel fulfillment as we do them. A [2015 study](#) examined factors that lead to SOC analyst burnout. The researchers found four factors that can lead to burnout if they're *not* present: possessing the right skills to do the job, feeling empowered to perform work efficiently, applying creativity to new scenarios and seeing a path for intellectual growth.

When analysts in the study were empowered and given incentive to engage with automation, they could be more creative through two paths. Automation took care of repeated tasks, so the analysts could pursue more fun and challenging cases. Working with developers to build the tool also tapped into their creativity. These changes in turn lead to more chances for intellectual growth, reducing the risk of burnout and creating a healthier work space.

Building Trust to Create a Cycle of Trust

Achieving this vision requires a crucial element: trust. Fear is a natural reaction to adding automation. Experts fear AI could take away their jobs in cybersecurity. Giving teams time to audit new systems is critical to building trust.

Before installing AI/ML, the machine should be put into simulation mode, allowing the team to audit how it performs. When nothing breaks and the routine work gives way to less noise, their confidence grows. Auditing gives teams time to adjust to a system that should lead to job satisfaction, not fear. And the auditing process should be done multiple times. Conducting short, daily audits ensures that if anything does go wrong, the team will catch it.

Teaching the machine on an ongoing basis creates a virtuous cycle of people being able to trust it and the machine performing at a higher level. AI learns from people and people learn from AI in a feedback loop that makes the team more efficient — and creates a stronger cybersecurity posture for the business overall.

As noted by the [2020 Cost of a Data Breach Report](#), “the effectiveness of security automation in reducing the average cost of a data breach continued to grow” over the past three years.

When it comes to building a healthy SOC and more fulfilling jobs in cybersecurity, AI/ML should be deployed in ways that first improve analysts’ day-to-day work. It’s worth stressing the point: [people are the most important element](#) in cybersecurity, and moving to a [modern SOC](#) starts with making the job better for them.

The post [How AI Can Make Cybersecurity Jobs Less Stressful and More Fulfilling](#) appeared first on [Security Intelligence](#).

Source: <https://securityintelligence.com/posts/how-ai-makes-jobs-in-cybersecurity-less-stressful/>

8. Be Very Sparing in Allowing Site Notifications

An increasing number of websites are asking visitors to approve “notifications,” browser modifications that periodically display messages on the user’s mobile or desktop device. In many cases these notifications are benign, but several dodgy firms are paying site owners to install their notification scripts and then selling that communications pathway to scammers and online hucksters.



Notification prompts in Firefox (left) and Google Chrome.

When a website you visit asks permission to send notifications and you approve the request, the resulting messages that pop up appear outside of the browser. For example, on Microsoft Windows systems they typically show up in the bottom right corner of the screen — just above the system clock. These so-called “push notifications” rely on [an Internet standard](#) designed to work similarly across different operating systems and web browsers.

But many users may not fully grasp what they are consenting to when they approve notifications, or how to tell the difference between a notification sent by a website and one made to appear like an alert from the operating system or another program that’s already installed on the device.

This is evident by the apparent scale of the infrastructure behind a relatively new company based in Montenegro called **PushWelcome**, which advertises the ability for site owners to monetize traffic from their visitors. The company’s site currently is [ranked by Alexa.com](#) as among the top 2,000 sites in terms of Internet traffic globally.

Website publishers who sign up with PushWelcome are asked to include a small script on their page which prompts visitors to approve notifications. In many cases, the notification approval requests themselves are deceptive — disguised as prompts to click “OK” to view video material, or as “CAPTCHA” requests designed to distinguish automated bot traffic from real visitors.

Best Web Push Solutions for Publishers Worldwide

Highest Push Notification payout rates for website owners, small publishers, high volume site owners.

100% 24/7

So much inventory going on, we ensure your traffic gets all relevant push notifications around the clock in all GEOS. We also make sure that you get the quality you deserve.

Flexible and On-time Payments

Your payments will be always on time and you can reinvest that money again, and earn even more. Need help with how to do that? Ping us.

Best High Converting Offers

Only the best and highly converting content will be served through our Push Monetization solutions. Our experience in the industry helped us pick the best for you.

Competitive Rates

In accordance with your content we will provide the best possible solutions. We know that you are here for the cash and we'll get you cash, and help you with getting most from your website

Easy Integration

It is really that simple. Register, create a tag and add it inside your website's head tag. This tag requests the user's permission to receive Push notifications, and that's it.

Everything in One Place

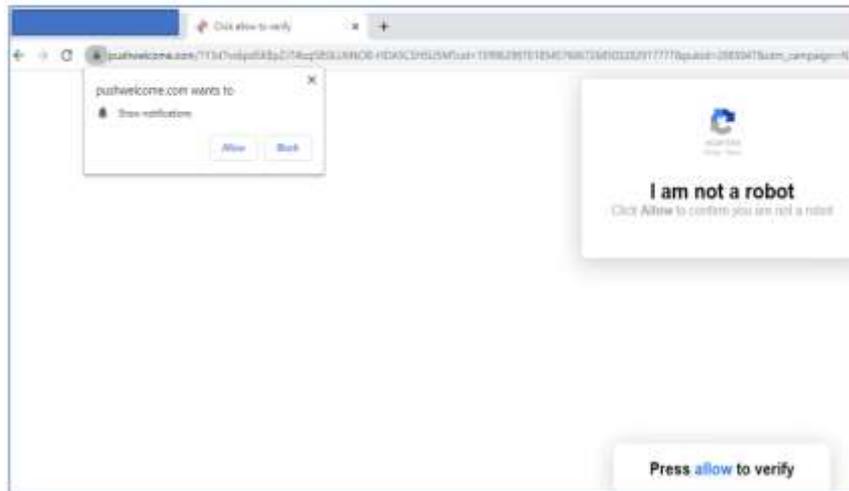
Edit, optimize, track - everything in one place. We have created such a system where you can do all of this from one single platform and save yourself a lot of time.

An ad from PushWelcome touting the money that websites can make for embedding their dodgy push notifications scripts.

Approving notifications from a site that uses PushWelcome allows any of the company's advertising partners to display whatever messages they choose, whenever they wish to, and in real-time. And almost invariably, those messages include misleading notifications about security risks on the user's system, prompts to install other software, ads for dating sites, erectile dysfunction medications, and dubious investment opportunities.

That's according to [a deep analysis](#) of the PushWelcome network compiled by [Indelible LLC](#), a cybersecurity firm based in Portland, Ore. **Frank Angiolelli**, vice president of security at Indelible, said rogue notifications can be abused for credential phishing, as well as foisting malware and other unwanted applications on users.

"This method is currently being used to deliver something akin to adware or click fraud type activity," Angiolelli said. "The concerning aspect of this is that it is so very undetected by endpoint security programs, and there is a real risk this activity can be used for much more nefarious purposes."



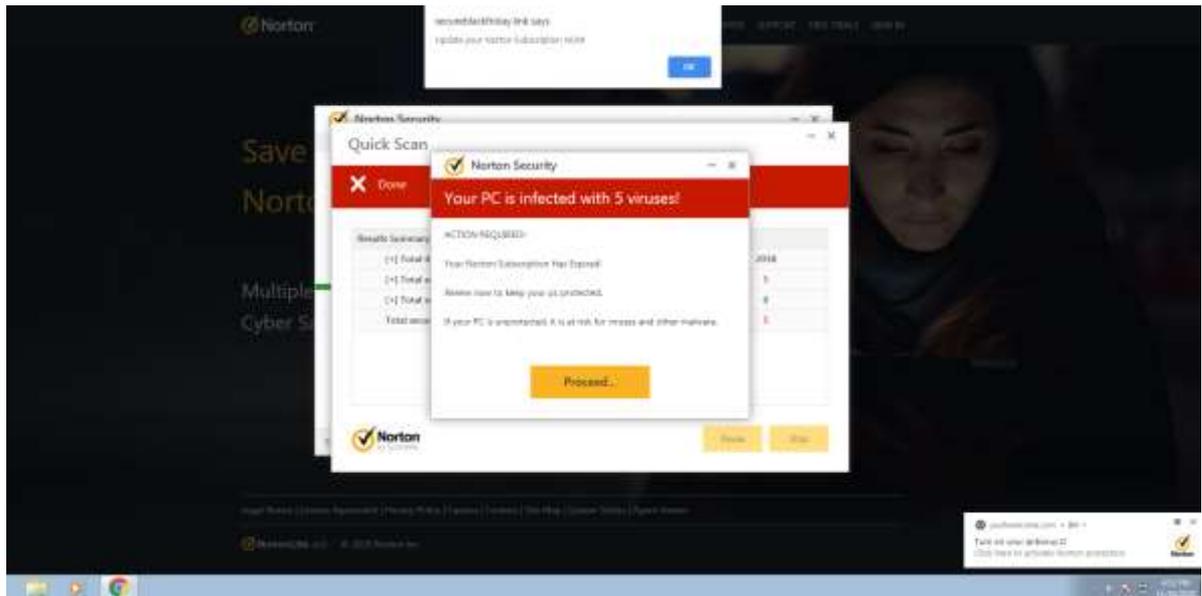
Sites affiliated with PushWelcome often use misleading messaging to trick people into approving notifications.

Angiolelli said the external Internet addresses, browser user agents and other telemetry tied to people who've accepted notifications is known to PushWelcome, which could give them the ability to target individual organizations and users with any number of fake system prompts.

Indelible also found browser modifications enabled by PushWelcome are poorly detected by antivirus and security products, although he noted Malwarebytes reliably flags as dangerous publisher sites that are associated with the notifications.

Indeed, Malwarebytes' **Pieter Arntz** warned about malicious browser push notifications [in a January 2019 blog post](#). That post includes detailed instructions on how to tell which sites you've allowed to send notifications, and how to remove them.

KrebsOnSecurity installed PushWelcome's notifications on a brand new Windows test machine, and found that very soon after the system was peppered with alerts about malware threats supposedly found on the system. One notification was an ad for **Norton** antivirus; the other was for **McAfee**. Clicking either ultimately led to "buy now" pages at either Norton.com or McAfee.com.



Clicking on the PushWelcome notification in the bottom right corner of the screen opened a Web site claiming my brand new test system was infected with 5 viruses.

It seems likely that PushWelcome and/or some of its advertisers are trying to generate commissions for referring customers to purchase antivirus products at these companies. McAfee has not yet responded to requests for comment. Norton issued the following statement:

“We do not believe this actor to be an affiliate of NortonLifeLock. We are continuing to investigate this matter. NortonLifeLock takes affiliate fraud and abuse seriously and monitors ongoing compliance. When an affiliate partner abuses its responsibilities and violates our agreements, we take necessary action to remove these affiliate partners from the program and swiftly terminate our relationships. Additionally, any potential commissions earned as a result of abuse are not paid. Furthermore, NortonLifeLock sends notification to all of our affiliate partner networks about the affiliate’s abuse to ensure the affiliate is not eligible to participate in any NortonLifeLock programs in the future.”



Requests for comment sent to PushWelcome via email were returned as undeliverable. Requests submitted through the contact form on the company's website also failed to send.

While scammy notifications may not be the most urgent threat facing Internet users today, most people are probably unaware of how this communications pathway can be abused.

What's more, dodgy notification networks could be used for less conspicuous and sneakier purposes, including spreading fake news and malware masquerading as update notices from the user's operating system. I hope it's clear that regardless of which browser, device or operating system you use, it's a good idea to be judicious about which sites you allow to serve notifications.

If you'd like to prevent sites from ever presenting notification requests, [check out this guide](#), which has instructions for disabling notification prompts in Chrome, Firefox and Safari. Doing this for any devices you manage on behalf of friends, colleagues or family members might end up saving everyone a lot of headache down the road.

Source: <https://krebsonsecurity.com/2020/11/be-very-sparing-in-allowing-site-notifications/>

9. Google's free services are now phishing campaign's best friends

Threat actors are abusing Google's free productivity tools and services to create convincing phishing campaigns that steal your credentials or trick you into installing malware.

Google offers a wide array of free software and services that allow users to create documents, spreadsheets, online forms, and free websites. These tools are used by students, teachers, consumers, and the enterprise as an easy way to share documents, conduct surveys, or even create sites for free.

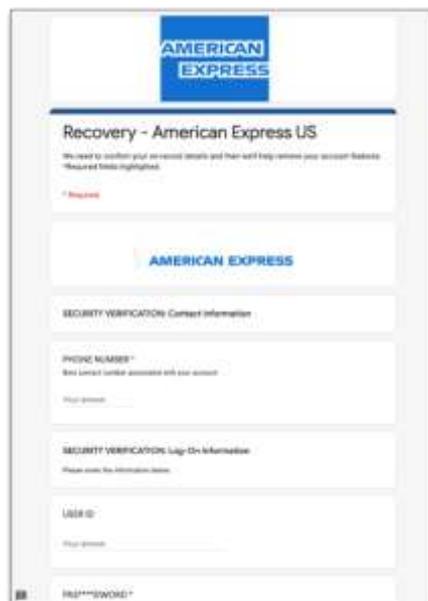
Unfortunately, if a service is free for us, it is also free for threat actors to abuse them as they see fit.

Threat actors abuse Google services for free

In a new report by email security firm Armorblox, researchers illustrate how threat actors are creating elaborate phishing campaigns using Google services that not only look convincing but also evade detection.

The first Google tool we will look at is the free form creation service called Google Forms that lets anyone create free online surveys that can then be sent to other users.

Threat actors, though, are abusing Google Forms to create elaborate forms that attempt to steal your credentials, like the fake American Express account recovery form below. Threat actors can then collect any submitted information at a later date.

A screenshot of a phishing form titled "Recovery - American Express US". The form features the American Express logo at the top. Below the title, there is a sub-header "Recovery - American Express US" and a small note: "We need to confirm your account details and then we'll help restore your account details. *Required fields highlighted." Below this, there is a "Required" label. The form contains several input fields: "PHONE NUMBER*" with a sub-note "This cannot be a number associated with our account", "SECURITY VERIFICATION: Consent information", "SECURITY VERIFICATION: Log-In Information" with a sub-note "Please enter the information below.", "USER ID:", and "PASSWORD*" (partially obscured by a password strength indicator).

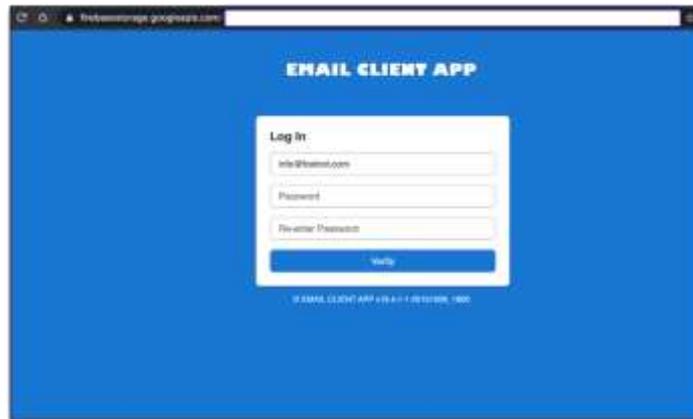
American express phishing form on Google Forms

Source: Armorblox

Google Firebase is a developer platform used to create mobile and web applications hosted in the cloud.

Threat actors are using Firebase to create phishing landing pages that can include images, dynamic content, and process forms. As Firebase pages utilize a generic <https://firebasestorage.googleapis.com> URL, Armorblox states they will not be "blocked by any security filters due to its inherent legitimacy."

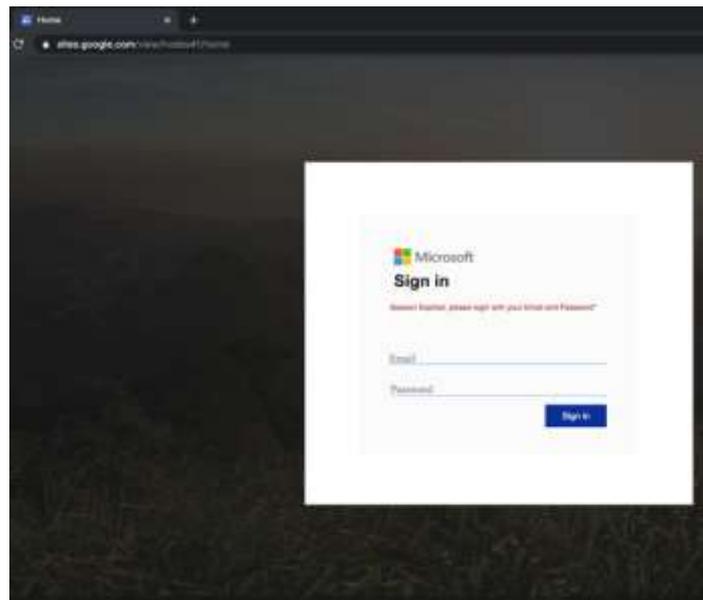
Below you can see a phishing email login form created on Firebase.



*Phishing form created with Google's Firebase service
Source: Armorblox*

Google offers a free web hosting platform called Google Sites that allows users to create simplistic web sites that are served from the sites.google.com domain.

In an example shared by Armorblox, we can see a Google Sites page that hosts a fake Microsoft sign-in form to steal a user's Microsoft account credentials.



*Google Sites phishing landing page
Source: Armorblox*



*BazarLoader Google Docs phishing page
Source: BleepingComputer*

While this report focused on the abuse of Google services, threat actors also utilize free services from other companies, including Dropbox, Canva, and Azure.

To protect yourself from phishing scams like these, Armorblox recommends that you:

Follow 2FA and password management best practices

Subject sensitive emails to rigorous eye tests, especially when related to money.

Create your own lines of authentication

Augment native email threat detection with additional controls

Even if you follow all of these recommendations, it is critical to treat all emails with links and attachments as suspicious.

Don't simply click on links or open attachments, instead scan them first or check with your network administrator if you're not sure. It is also always good to call the sender by phone to confirm if they sent the email.

Just be sure not to use the phone number listed in the email, as it could be the threat actor's number instead.

Source: <https://www.bleepingcomputer.com/news/security/google-s-free-services-are-now-phishing-campaign-s-best-friends/>

10. IBM CISO Perspective: Zero Trust Changes Security From Something You Do to Something You Have

As the chief information security officer (CISO) for IBM, I'm often asked by peers and colleagues, "What do you think of Zero Trust?"

Or, perhaps more often, "What strategies are you using to keep IBM protected?"

First, many vendors in the security industry are looking at zero trust security from the wrong perspective. Security isn't something you can just 'do.' Sure, you may be able to buy security tools or products. As a security professional, you might have a lot of experience at adjusting firewall or provisioning policies, or have specialized training to investigate incidents. While these things can be helpful in applying security to your organization's business practices, they are not really advancing the business in a secure way.

That is an important distinction and provides the basis of our view of [zero trust](#). Zero trust isn't something you can buy or implement. It's a philosophy and a strategy. And to be frank, at IBM, we wouldn't even characterize zero trust as a security strategy. It's an IT strategy done securely.

Cloud First — More than an IT Strategy

Consider this. For the last several years, our IT strategy has followed a simple rule: cloud first. Everything we build or buy — from our marketing tools to our developer technology to our collaboration applications — is delivered as a service or is available to be hosted on our public cloud. This strategy addresses two critical business objectives:

- **Enabling end-user productivity.** First and foremost, end-user productivity is paramount. We need to connect our employees to the tools they need in the most fluid and cost-effective way possible. Moving everything to the cloud allows us to provide a consistent and seamless experience for our users no matter where they are or what device they use. The pandemic provided a great test of our strategy and, generally speaking, it was pretty painless. Our employees were able to continue working with little to no disruption.
- **Protecting critical data.** Moving everything to the cloud also helps us from a security standpoint. Delivering employee tools and applications from the cloud allows us to be independent of our internal network. In turn, we can treat our internal network as a hostile environment. This allows us to put in more controls to help protect our most sensitive data.

A Deeper Dive into Securing Our Users

So how do we provide our users with seamless, fluid experience no matter where they are and protect our most critical data at the same time? Here are my areas of focus:

Identity as Essential Control Point for Authentication

Our centralized enterprise [identity project](#) is a cloud-based program that securely connects our users to the resources they need. The basic elements of this program are:

- Providing single sign-on (SSO) to all applications using IBM Security Verify with OpenID Connect, Security Assertion Markup Language and other open standards. This helps employees limit the passwords they need to manage.
- Deploying passwordless authentication wherever possible using FIDO2, QR codes and device trust. This makes it easy for employees to log in, while at the same time offering more security than relying solely on passwords.
- Supporting modern verification factors using the [IBM Security Verify](#) solution for quicker, more convenient multifactor authentication (MFA) experiences with additional transaction information for users to correlate requests back to what they see on screen, reducing phishing attempts.

Device Flexibility Underpinned With Integrated Security Capabilities

A key tenet of our IT and security strategy is flexibility, so we offer our users a choice of devices to work from. This requires us to take extra steps — more integration — ensuring not only the integrity of the device, but also how it is being used.

We rely on [user risk management](#) technologies from [IBM Security MaaS360](#), as well as endpoint visibility tools like JAMF and Intune to help us consider the risks of the endpoint at the time of access. These are a key part of our project and provide critical data to isolate endpoints in the event of a compromise.

Automation to Quickly Respond to Incidents at the Endpoint

While the practices outlined above go a long way toward insulating our most sensitive data, we know that it's not enough. When nation-states attack, we have only minutes to respond before they move laterally from the endpoint to another area deeper within the organization.

As highlighted above, we offer our users flexibility in their devices; this translates to hundreds of thousands of endpoints to monitor. Using integrated endpoint detection and response, we can identify a threat and isolate or kill the device within minutes before the attackers have a chance to move. In addition to protection, we are using these use cases

to increasingly automate the response process. This helps us intercept attacks at an earlier stage, which significantly decreases investigation time. It also allows our highly trained analysts to focus on the most significant risks.

Zero Friction, Zero Trust

At IBM, we are committed to [building and maintaining trusted relationships](#) with our customers. This trust is built on an expectation for delivering innovation, as well as protecting and safeguarding our intellectual property, customer data and employee information. For us, this requires a comprehensive IT strategy executed securely.

This requires flexibility to empower our lines of business to access and use the tools they need to create, deliver and market the innovations our customers expect. It means providing a stable, reliable environment for teams and individuals to connect to the applications and technologies they need to do their job — even in the midst of a pandemic. And perhaps most importantly, our approach is underpinned with multi-faceted security integrated tightly into the daily operations of our business, providing ambient protection of both our users and our data.

The post [IBM CISO Perspective: Zero Trust Changes Security From Something You Do to Something You Have](#) appeared first on [Security Intelligence](#).

Source: <https://securityintelligence.com/posts/ibm-ciso-perspective-zero-trust-changes-security/>

11. Passwords exposed for almost 50,000 vulnerable Fortinet VPNs

A hacker has now leaked the credentials for almost 50,000 vulnerable Fortinet VPNs.

Over the weekend a hacker had posted a list of one-line exploits for CVE-2018-13379 to steal VPN credentials from these devices, as reported by BleepingComputer.

Present on the list of vulnerable targets are IPs belonging to high street banks, telecoms, and government organizations from around the world.

Leaked files expose usernames, passwords, unmasked IPs

The exploitation of critical FortiOS vulnerability CVE-2018-13379 lets an attacker access the sensitive "sslvpn_websession" files from Fortinet VPNs.

These files contain session-related information, but most importantly, may reveal plain text usernames and passwords of Fortinet VPN users.

Today, threat intelligence analyst Bank_Security has found another thread on the hacker forum where a threat actor shared a data dump containing "sslvpn_websession" files for every IP that had been on the list.

As observed by BleepingComputer, these files reveal usernames, passwords, access levels (e.g. "full-access"), and the original unmasked IP addresses of users connected to the VPNs.



Hacker leaks sslvpn_websession files containing credentials from almost 50,000 Fortinet VPNs

Source: Twitter

The new data set posted on the forum is merely a 36 MB RAR archive, but when decompressed, expands over 7 GB, at the time of our testing.

The exposure of passwords in these files means, even if the vulnerable Fortinet VPNs are later patched, these credentials could be reused by anyone with access to the dump in credential stuffing attacks, or to potentially regain access to these VPNs.



Folder structure of Fortinet leaked password dump

Leaked folder structure with a separate list of vulnerable Fortinet devices in Pakistan
Source: BleepingComputer

While the threat actor's motivations for this second, expansive leak aren't clear, BleepingComputer did notice, the newly leaked archive has lists marked pak separating out Pakistan-based VPN IPs and corresponding "sslvpn_websession" files from the large 49,000+ VPN data set.

Additionally enclosed is an image file titled, "f**k israel.jpg" which is a "Yes we can" Adolf Hitler poster created in the style of Obama's 2008 presidential campaign poster.

To make matters worse, the credential dump is being reposted on other forums and chats.

Fortinet repeatedly tried to warn customers

This week Fortinet told BleepingComputer, ever since the public disclosure of the critical Path Traversal vulnerability (CVE-2018-13379) last year, the company had repeatedly alerted its customers, encouraging them to patch the vulnerable FortiOS instances.

"The security of our customers is our first priority. In May 2019 Fortinet issued a PSIRT advisory regarding an SSL vulnerability that was resolved, and have also communicated directly with customers and again via corporate blog posts in August 2019 and July 2020 strongly recommending an upgrade," a Fortinet spokesperson told BleepingComputer.

Despite these measures, the critical bug has been extensively exploited in the wild due to a lack of patching.

The same flaw was leveraged by attackers to break into US government elections support systems, as reported by BleepingComputer.

Earlier this year, nation-state threat actors had weaponized the vulnerability to compromise networks and deploy ransomware.

"In the last week, we have communicated with all customers notifying them again of the vulnerability and steps to mitigate. While we cannot confirm that the attack vectors for this group took place via this vulnerability, we continue to urge customers to implement the upgrade and mitigations. To get more information, please visit our updated blog and immediately refer to the May 2019 [PSIRT] advisory," concluded Fortinet.

Network administrators and security professionals are therefore encouraged to patch this severe vulnerability immediately.

As a safeguard, Fortinet VPN users should change their passwords immediately both on the VPN devices, and any other websites where the same credentials were used.

Source: <https://www.bleepingcomputer.com/news/security/passwords-exposed-for-almost-50-000-vulnerable-fortinet-vpns/>

12. Sophos alerts customers of info exposure after security breach

British cybersecurity and hardware company Sophos has emailed a small group of customers to alert them that their personal information was exposed following a security breach discovered on Tuesday.

The exposed customer data was accessible to unauthorized parties due to a misconfigured "tool" used by the company to store information by users who reached out to the company's support team.

Only a small subset of customers affected

"On November 24, 2020, Sophos was advised of an access permission issue in a tool used to store information on customers who have contacted Sophos Support," the company said in the notification email.

"As a result, some data from a small subset of Sophos customers was exposed. We quickly fixed the issue."

Sophos did not provide any information on who discovered and disclosed the insecure storage tool or on the exact number of customers who had their personal info exposed due to this security breach.

The exposed data includes customers' first and last names, email addresses, and their contact phone number if it was provided to Sophos Support.

The company also said that the customer support information is no longer exposed after remediation measures were taken to stop the data exposure.

On November 24, 2020, Sophos was advised of an access permission issue in a tool used to store information on customers who have contacted Sophos Support. As a result, some data from a small subset of Sophos customers was exposed. We quickly fixed the issue.

Your information was exposed, but due to remediation measures we have taken, your data is no longer exposed. Specifically, first name, last name, email address and, where provided, a contact phone number.

Sophos breach notification

"At Sophos, customer privacy and security are always our priority," the cybersecurity firm added. "We are contacting all affected customers."

"Additionally, we are implementing additional measures to ensure access permission settings are continuously secure."

Not the first security incident this year

Earlier this year, Sophos fixed a zero-day SQL injection vulnerability in their XG Firewall following reports that hackers were actively exploiting it in attacks.

A new Trojan malware, dubbed Asnarök by Sophos researchers, exploited the zero-day to try and steal firewall usernames and hashed passwords from XG Firewall users starting with April 22, 2020.

The same Sophos XG firewall zero-day was also exploited in failed attempts to deliver Ragnarok Ransomware payloads onto companies' Windows systems.

Update: A Sophos spokesperson told BleepingComputer that only "a small subset was affected in no specific region" and that "Sophos quickly fixed the issue."

Source: <https://www.bleepingcomputer.com/news/security/sophos-alerts-customers-of-info-exposure-after-security-breach/>

13. The Future of Cybersecurity: How to Prepare for a Crisis in 2020 and Beyond

When it comes to the future of cybersecurity, an ounce of prevention is worth far more than a pound of cure. According to the Ponemon Institute and IBM Security's 2020 Cost of a Data Breach Report, enterprises that designated an incident response (IR) team, developed a cybersecurity incident response plan (CSIRP) and tested their plan using tabletop exercises or simulations, saved an average of \$2 million in data breach costs. These savings were compared to companies that didn't take these preparatory steps.

To improve preparedness — and bolster security teams' confidence — it's essential to move beyond creating flat, static incident response plans and instead use brief crisis simulation exercises that closely mimic what would take place in a real-world attack today. Here are five key ways to achieve this.

2020 Cybersecurity Trends

The future of cybersecurity brings with it a lot of changes, some of which we can predict today. Not all incident response planning and cyber crisis preparedness exercises are created equal, as a new Osterman Research study highlights. In fact, businesses tend not to be prepared for the most rapidly expanding threats, including ransomware. Ransomware's prevalence increased by 365% between Q2 2018 and Q2 2019, and then grew by another 148% during the COVID-19 crisis. Teams also tend to work from too general of cybersecurity incident response plan templates, failing to include attack-specific playbooks, realistic simulations or multiple varied attack examples.

It's the nature of cybersecurity in 2020: attackers' strategies and techniques change rapidly. According to IBM Security X-Force Incident Response, which has seen an explosive increase in ransomware attacks this year, particularly in Q2 of 2020, today's attackers are very agile. Ransom demands are increasing by leaps and bounds while attackers narrow their focus to victims, such as manufacturers who can incur millions of dollars in losses from a day-long halt in work, and thus have little tolerance for downtime.

Threat actors are also blending new data theft-based extortion tactics into ransomware attacks, stealing sensitive company information and threatening to make it public if their victims don't pay for the decryption key. These altered tactics demand revised incident response and crisis recovery plans, but many security teams aren't keeping pace.

There's a widespread tendency to review, update and test enterprise-wide incident response plans slowly while the future of cybersecurity becomes now. Meanwhile, attackers evolve more quickly. This likely contributes to the lack of confidence displayed

by the senior leaders surveyed in the Osterman Research report. Nearly 40% of respondents said they were not confident their teams would be able to handle a data breach if one were to occur that week.

1. Build a Cybersecurity Incident Response Plan

First of all, it is essential to have a formal plan. Among the IT and security professionals surveyed in IBM Security's 2020 Cyber Resilient Organization Report, those designated as "high performing" were more than twice as likely as the average entity to have a cybersecurity incident response plan (CSIRP) for their whole enterprise. What's notable about these high performers, though, is their plans were more likely to be applied the same across the entire company. They were also far more likely to have developed response plans for specific attacks than the average responder.

Consistent training across the business or other entity is a mark of buy-in from leadership on down to front-line employees. An effective security awareness training program can help to foster this mindset, as can a commitment from the C-suite to regularly plan, practice and improve cybersecurity crisis response procedures.

2. A CSIRP Is a 'Living Document'

The 2020 Cyber Resilient Organization Report found that across industries, organizations that don't review and update their CSIRPs often are more likely to face disruption to IT and business processes in case of a breach. Nonetheless, only 7% of participants in the survey review and update their CSIRPs on a quarterly basis. A significant number (40%) don't have any set schedule at all for preparing for the future of cybersecurity in this way.

Because today's threat landscape is evolving so quickly, the only way to prepare adequately for the specific attack types and vectors most likely to impact your individual enterprise is to incorporate threat modeling into your IR planning. In turn, this is impossible to do if you aren't updating your plans frequently. Ransomware tactics — which have grown in prevalence by nearly 70% in recent years — are speedy and change fast.

"If you did your ransomware training in January, you're likely five ransomware techniques behind the curve now," says James Hadley, CEO of Immersive Labs.

3. Thoroughly Test Any Plan

According to the Osterman Research report, a majority of security leaders (61%) believe that having an IR plan in place is the single most effective method to prepare for a future attack. But as the Cost of a Data Breach Report reveals, practicing for a real-life crisis is equally if not more important. The average total cost of a data breach for companies that tested their IR plan using tabletop exercises or simulations was \$2 million less than the average breach cost for groups that did not test their plans.

Like updating the IR plan, running tabletop examples or other simulations tends to take place far too rarely to be as effective as they could be. More than one-third of groups surveyed by Osterman say they conduct tabletop exercises, fire drills or other training every one to two years. This simply isn't enough to present realistic scenarios based on the techniques currently favored by attackers, not to mention those coming in the future of cybersecurity.

4. All Methods of IR Testing Are Not Created Equal

There are intrinsic problems with the nature and format of tabletop exercises. The most common method for conducting them (employed 65% of the time, according to Osterman Research) involves discussion and review of PowerPoint slides. Stakeholders tend to find these boring, and they often fail to convey the importance of psychological readiness for an attack. They also fail to generate increased buy-in from key stakeholders or raise awareness.

Many times, senior business leaders simply don't show up for these sessions. In some cases (25% of the time, according to Osterman Research), even senior cybersecurity leadership fails to attend.

Despite that actual cybersecurity crises impact nearly every area of the business, with legal teams, marketing and PR and executive leadership having critical roles to play in responding. And, it's difficult to assemble teams from across the enterprise for tabletop practice sessions, despite that an actual cybersecurity crisis impacts nearly every area of the business.

Furthermore, there's an inherent trade-off within tabletop exercise planning. The more detailed and specific the exercise, the more useful it is for getting people ready for a real-world incident. However, the more numerous, detailed and specific the cases covered within a tabletop exercise, the longer that exercise will take. A major time commitment makes it more difficult to schedule and more onerous to conduct. A key challenge is to balance frequency with depth.

5. Try Online Crisis Simulation Training

There's a great need for crisis training that's more effective than what most providers currently have in place. One emerging product offering is providing brief, gamified crisis simulations online. These exercises are quick to complete, can be tailored to address an enterprises' most pressing current risks and run on demand. Remote workers, who otherwise tend to be neglected during in-office simulations and larger scale practical training sessions, can access them. And they are less burdensome than conducting tabletop exercises. Therefore, online crisis examples may generate increased buy-in across the enterprise, even among non-technical staff.

Prepare for the Future of Cybersecurity

There's no doubt that the future of cybersecurity will depend on new technologies. But not all of these technologies will involve collecting data, monitoring or controls on IT infrastructures. Some will instead assist in improving the way humans respond in a crisis. Blocking cyberattacks and preventing data breaches requires both technology and human buy-in.

Source: <https://securityintelligence.com/articles/future-of-cybersecurity-how-to-prepare-for-crisis-2020-and-beyond/>

If you want to learn more about ASOC and how we can improve your security posture, contact us at: tbs.sales@tbs.tech

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK BUSINESS SERVICES's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK BUSINESS SERVICES is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.