telelink
BUSINESS SERVICES

Advanced Security Operations Center
Telelink Business Services
www.tbs.tech

Monthly Security Bulletin

December 2021

This security bulletin is powered by Telelink Business Services'

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

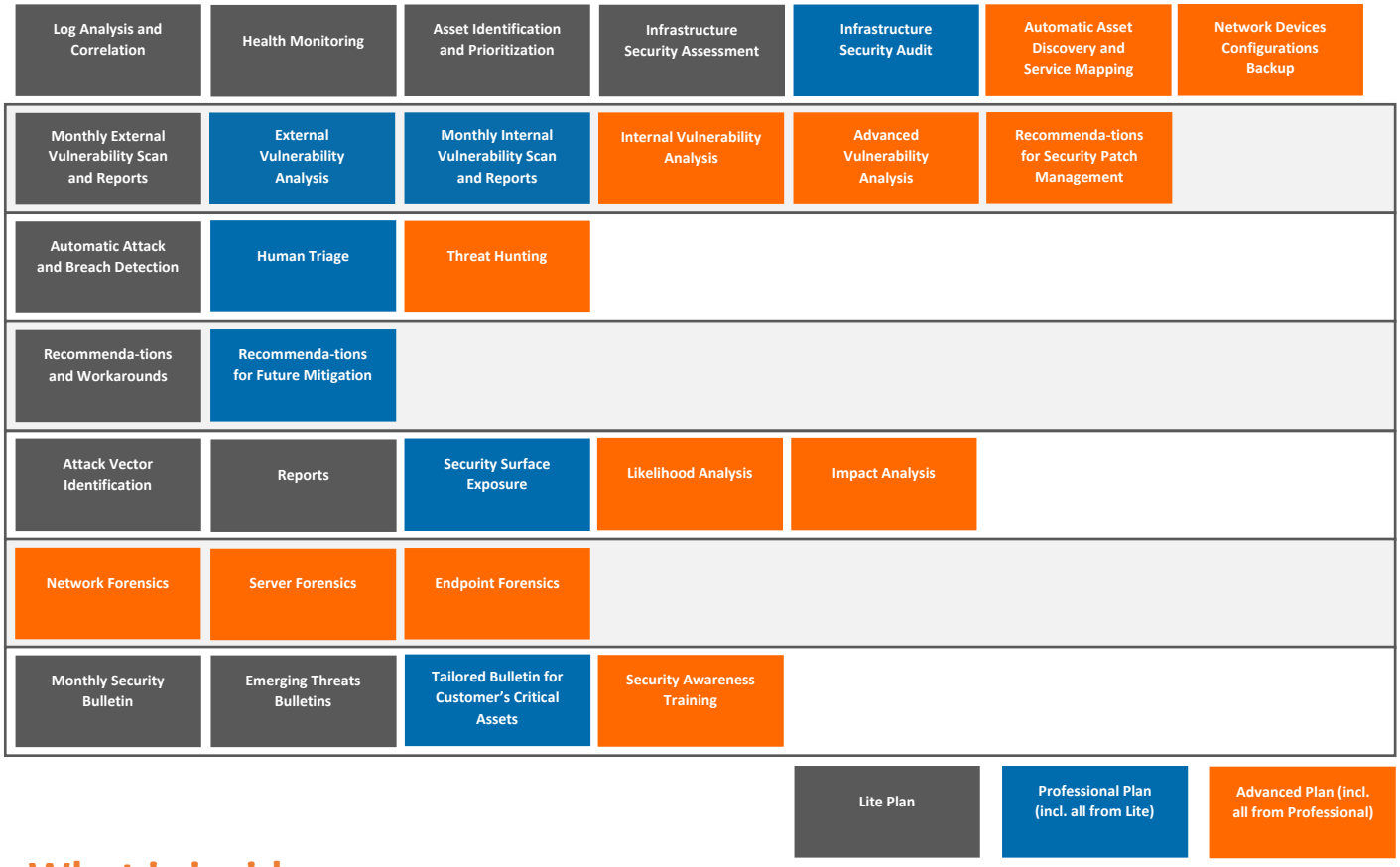
Start to mitigate cyber threats and minimize the risk!

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!



What is inside:

- Infrastructure Security Monitoring – the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management – get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection – get data from state-of-the-art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations – get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis – get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis – in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness – be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link

Table of Contents

1. Microsoft Defender for Windows is getting a massive overhaul

Microsoft Defender for Windows is getting a massive overhaul allowing home network admins to deploy Android, iOS, and Mac clients to monitor antivirus, phishing, compromised passwords, and identity theft alerts from a single security dashboard.

In the past, antivirus solutions were very much a single PC application, where each device got its own protection, but none of the devices spoke to each other.

With this setup, if one device detected malware, only the person using the device would know about it, rather than providing a centralized reporting dashboard.

As home networks became increasingly more complicated, connected, and diverse, antivirus vendors started to offer stripped-down versions of their enterprise products that allowed a home admin to manage all of their devices from a single dashboard.

Microsoft's full-featured home security suite

For the past few years, Microsoft has been focusing on the enterprise's security while leaving Windows 10 consumers with the passable but fairly generic built-in Microsoft Defender antivirus software.

Based on a new Microsoft Defender Preview app added to the Microsoft Store last week, this is all about to change, with Microsoft building what appears to be a full-featured home security suite for Windows 11, Windows 10, iOS, Android, and macOS.

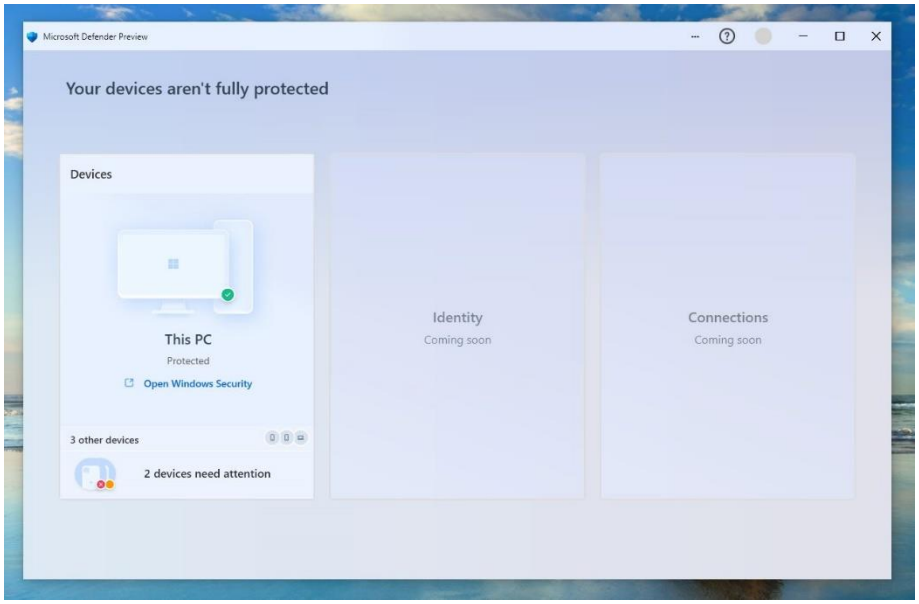
"Microsoft Defender is a security application that gives you peace of mind. Through our personalized dashboard, you can view the security posture of your Windows device and other connected devices (Mac, iOS, and Android) all in one place," reads the Microsoft Defender Preview app description.

This new preview is codenamed 'Gibraltar' internally as it is currently restricted to Microsoft employees.

However, BleepingComputer found strings in the executables that indicate that the new security solution will include antivirus, phishing protection, password breach detection, identity theft monitoring, security recommendations, and more.

Home admins will add other family members to their personal dashboard using email or QR code invites. These invites will likely allow a device to install an iOS, Android, Windows, or macOS agent that automatically enrolls in the family's security dashboard.

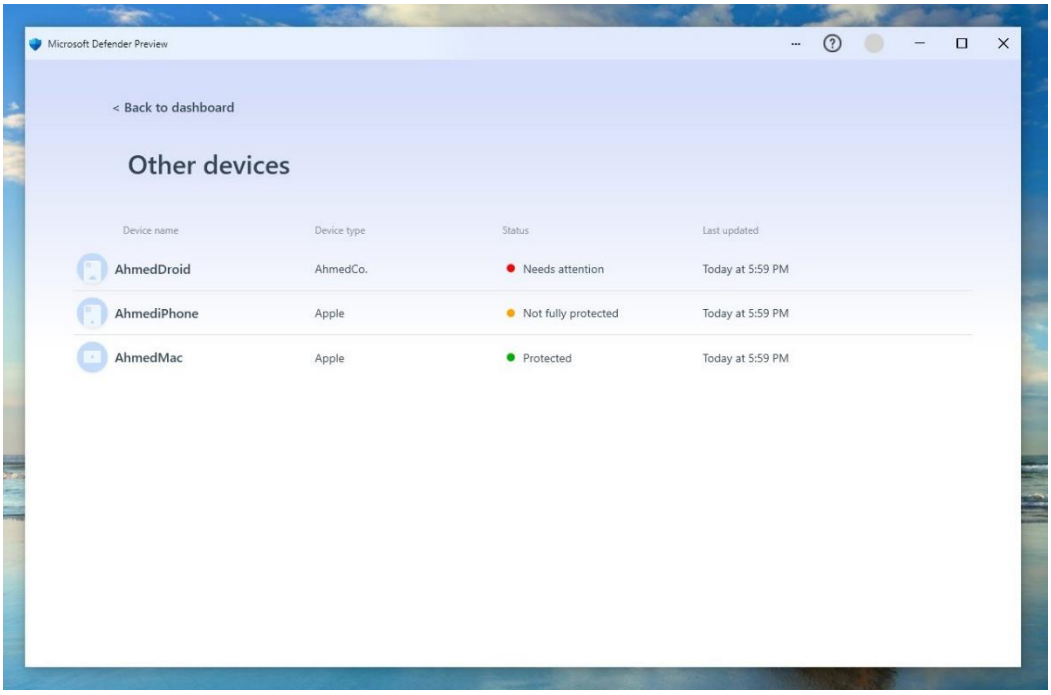
Windows software developer Ahmed Walid patched the application to bypass authentication, allowing us to get a glimpse of how the new Microsoft Defender security dashboard will look.



Microsoft Defender Preview dashboard
Source: Walid

As you can see above, the dashboard will allow you to view health alerts for devices, with Identity and "Connections" monitoring coming soon. In addition, the Identity Theft Monitoring feature will support child, and adult subscriptions from API calls found in the Microsoft Defender Preview.

Using their "personal dashboard," home network administrators can monitor all enrolled devices for "health" alerts that may include compromised passwords, malware alerts, or identity theft issues.



Summary of monitored devices
Source: Walid

It is unclear when the Microsoft Defender Preview will be available to test, but it will likely come to Windows 10 and Windows 11 Insiders first in the coming months.

BleepingComputer has contacted Microsoft with further questions about this new feature and will update the article if we receive a response.

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-for-windows-is-getting-a-massive-overhaul/

2. Over 30,000 GitLab servers still unpatched against critical bug

A critical unauthenticated, remote code execution GitLab flaw fixed on April 14, 2021, remains exploitable, with over 50% of deployments remaining unpatched.

The vulnerability is tracked as CVE-2021-22205 and has a CVSS v3 score of 10.0, allowing an unauthenticated, remote attacker to execute arbitrary commands as the 'git' user (repository admin).

This vulnerability gives the remote attacker full access to the repository, including deleting, modifying, and stealing source code.

Exploitation in the wild

Hackers first started exploiting internet-facing GitLab servers in June 2021 to create new users and give them admin rights.

The actors used a working exploit published on GitHub on June 4, 2021, allowing them to abuse the vulnerable ExifTool component.

The threat actors do not need to authenticate or use a CSRF token or even a valid HTTP endpoint to use the exploit.

With the exploitation continuing to this day, researchers from Rapid7 decided to look into the number of unpatched systems and determine the scope of the underlying problem.

According to a report published by Rapid7, at least 50% of the 60,000 internet-facing GitLab installations they found are not patched against the critical RCE flaw fixed six months ago.

Moreover, another 29% may or may not be vulnerable, as the analysts couldn't extract the version string for those servers.

Admins need to update to one of the following versions to patch the flaw:

- 13.10.3
- 13.9.6
- 13.8.8

Any versions earlier than that and down to 11.9 are vulnerable to exploitation whether you're using GitLab Enterprise Edition (EE) or GitLab Community Edition (CE).

For more details on how to update GitLab, check out this dedicated portal.

To ensure that your GitLab instance isn't vulnerable to exploitation, you can check its response to POST requests that attempt to exploit ExifTool's mishandling of image files.

The patched versions still allow someone to reach out to ExifTool, but the response to the request should be a rejection in the form of an HTTP 404 error.

Source: *https://www.bleepingcomputer.com/news/security/over-30-000-gitlab-servers-still-unpatched-against-critical-bug/*

3. Squid Game Crypto Scammers Rip Off Investors for Millions

Anti-dumping code kept investors from selling SQUID while fraudsters cashed out.

Players in the Squid Game cryptocurrency market have been eliminated — at least their investment has — by what cryptocurrency watchers have called a classic "rug-pull" scam.

When SQUID tokens were first released last week, they were valued at a paltry $0.01 but promised entry into a game with the same premise as the Squid Game series from Netflix — players in desperate financial straits compete in a ruthless, deadly series of games for a shot at winning millions.

On Nov. 1 the price started escalating dramatically, but investors were blocked from selling SQUID by a so-called "anti-dumping mechanism." Meanwhile, scammers cashed out, according to complaints received by CoinMarketCap. SQUID's value peaked at $2,861.80 and dropped to zero within hours.

The intoxicating combination of a get-rich-quick cryptocurrency investment and the Netflix wild smash hit show Squid Game was just too much for some investors to resist, and estimates from Gizmodo peg potential losses from the scam at around $3,38 million.

Stop Sales, Spike Price

All it took to keep investors from selling was a simple piece of code, Joe Stewart, researcher with PhishLabs HelpSyst4ems, explained to Threatpost.

"All the rules of how a token can be bought and sold are contained in the smart contract code itself, since these tokens are traded on a decentralized 'automatic market-maker' contract," Stewart said. "Basically, it just needs an extra line of code in the transfer function to prohibit the swap from occurring in the 'sell' direction unless the transaction sender is the address controlling the contract (i.e. the developer who removed all the liquidity from the pool and absconded)."

CoinMarketCap reported viewing messages from SQUID administrators blaming issues on a compromise of their systems.

"Someone is trying to hack our project these days," CoinMarketCap reported the administrators said about the incident. "Now only the Twitter account but also our smart contract."

The Twitter account associated with the SQUID cryptocurrency has been "temporarily restricted for… unusual activity," and the squidgame.cash site is gone, according to the report.

'Nifty Scheme'

Purandar Das, president and co-founder at Sotero, called this an "electronic pump-and-dump scheme" in an email to Threatpost.

"It appears they may have come up with a very nifty scheme," Das wrote. "Adopting the brand of a very popular and current theme would have permitted them to cover themselves with a cloak of credibility. Combine that with the fear of missing out, they appear to have concocted a scheme to combine the Squid Game name with cryptocurrency."

Popular headlines and events, from COVID-19 to elections and holidays, have proven effectively popular ways for scammers to not only drum up interest but also hide the fraud in flurries of legitimate activity. That reality, coupled with renewed criminal interest in efforts to scam gamers and rip off cryptocurrency platforms, means that a fake Squid Game gaming crypto-scam seems practically predictable.

Das explained that in a market artificially rigged with only buyers, the price of SQUID was designed to dramatically spike at the opportune time for the scammers.

"Using digital currency also eliminates any fail-safes from kicking in," he added.

It's up to buyers and investors to beware of scams like these, researchers added.

Source: https://threatpost.com/squid-game-crypto-scammers-investors/175951/

4. Report: Cost of a Data Breach in Energy and Utilities

On average, the cost of a data breach rose by 10% from 2020 to 2021. The energy industry ranked fifth in data breach costs, surpassed only by the health care, financial, pharmaceutical and technology verticals, according to the 17th annual Cost of a Data Breach Report. Some energy cybersecurity measures can help reduce the cost of a data breach in a big way. For example, take a look at zero trust deployments, artificial intelligence and automation.

It's important to better understand data security in this growing and crucial field. Take a look at some recent data breaches that affected energy and utility providers. What data security risks and challenges are unique to these sectors?

What Is a Data Breach in the Energy and Utilities Industries?

The energy sector includes oil and gas companies, alternative energy producers and suppliers and utility providers such as electric companies. Energy cybersecurity breaches and failures can have tremendous impacts. They even go beyond the cost to the

companies that mine for oil or gas or provide energy to customers. After all, people rely on these services for nearly every aspect of life.

Compromised Password Leads to Gas Shortages

This type of problem joined the United States' many other challenges in spring 2021. An attacker gained remote access to the network of a major U.S. pipeline company via an employee's virtual private network (VPN). The VPN was not even in use at the time. However, it remained open for threat actors to use it as a gateway to the company's main network. The attacker found the password used to access the account on a list of leaked passwords on the dark web. Experts suggest that the employee may have used the same password on another account. A threat actor then stole it from that account and shared it online.

One week after the data breach, the threat actor sent a ransom note. In response, the company shut the pipeline down. They did so on purpose because they wanted to avoid an attack on their operational technology network. After all, these are the systems that control the physical flow of gasoline.

This happened to occur at the same time as increases in COVID-19 vaccinations and car travel across the U.S. Because of this, the resulting gasoline shortage led to long lines at gas stations and high oil prices. That in turn directly affected consumers' wallets just as many were beginning to return to work and recover financially amidst a global pandemic.

This shows the importance of educating employees on data protection and data security best practices. In particular, make sure to use unique passwords for every account.

San Francisco Utility Fined $2.7 Million

The rise in smart meters introduces new threats to utilities such as power companies. One San Francisco-based utility was saddled with a $2.7 million fine from federal security regulators for failing to protect confidential data, which included more than 30,000 pieces of information. A third-party contractor allegedly copied data from the utility's network to its own. From there, it was hosted online without a user ID or password.

Threats of ransomware and denial-of-service attacks are also a concern for utilities that implement smart meters and store customer data on their network. That's a big problem if that network falls out of the control of the utility.

Solar Devices Create Portal to Access the Grid

Cyber attacks and big data security concerns affect all kinds of energy companies. In 2019, the Department of Energy reports, threat actors breached the web portal firewall of a solar power utility. This caused operators to lose visibility for parts of the grid for 10 hours.

Devices such as solar photovoltaic inverters that connect to the internet to help manage the grid can become targets. In particular, attackers can take advantage if the company doesn't update and secure their inverter software.

What Is the Cost of a Data Breach for Energy and Utilities Companies?

The Cost of a Data Breach Report, which has grown into a leading benchmark report in the cybersecurity industry, shares that the average cost of a data breach in the energy industry is $4.65 million. The good news is this figure has dropped by 27.2% since 2020 when the average cost of a data breach in the industry was up to $6.39 million.

Risks and Challenges of Data Security

Social engineering, system intrusion and web application attacks made up 98% of energy data breaches in 2021. Social engineering, or phishing, attacks were the most common, although ransomware attacks continue to be a threat for the sector.

According to the Verizon report, the following data was stolen, lost or rendered inaccessible by ransomware most often:

- Login credentials
- Internal company data
- Personal data of employees and customers.

In 98% of all cases, the threat actors were not connected with the companies in any way; only 2% of attacks were internal breaches.

There's more good news, too. The threat of 'hacktivism', threat actors who operate because of causes such as environmentalism and sustainability, is on a steep decline. According to the IBM X-Force Threat Intelligence Index, these attacks dropped by 95% between 2015 and 2019. Of course, oil and gas companies could be the primary targets of such attacks. So, their decline frees up energy cybersecurity departments to focus their budget and attention on other threats.

The rise of employees working from home and accessing networks remotely also creates a growing threat. The IBM report discovered that the cost of a data breach rose by an average of $1.07 million when remote work was a factor. In situations where more than 50% of the workforce was remote, it took IT security experts an average of 58 days longer to detect and contain threats.

Taking proactive steps toward employee education regarding cybersecurity best practices can help mitigate risks. Make sure your people know how to reduce the risk of compromised credentials, which were responsible for 20% of all attacks, according to the

report. On top of that, train them to look out for the signs of social engineering and phishing.

Source: https://securityintelligence.com/articles/cost-data-breach-energy-utilities/

5. Fortinet Offers the Most Complete Work-from-Anywhere Security Solution

Over the past decade or so, technology has been steadily evolving to provide workers with more flexibility regarding the devices they use, the locations they can work from, and the resources they can access. BYOD and the cloud were the first steps for enabling people to work from anywhere. Then SaaS, combined with smarter endpoint devices and LTE/5G connectivity, transformed businesses, allowing them to compete more effectively in an increasingly digital marketplace.

While we were on pace to eventually embrace a true work-from-anywhere (WFA) strategy sometime in the next few years, the COVID-19 pandemic accelerated the need. And after a year, workers are now demanding that employers provide a WFA option. Forecast analysis from Gartner®1 indicates that "by the end of 2024, the change in the nature of work will increase the total available remote worker market to 60% of all employees, up from 52% in 2020." Also, according to Gartner2, "Organizations are facing a hybrid future, with 75% of hybrid or remote knowledge workers saying their expectations for working flexibly have increased." The challenge is how to deliver a hybrid work experience safely and productively.

The Security Challenges of a Hybrid Workforce

The challenge was that few organizations were prepared for extensive work-from-home when the pandemic hit. Workers were suddenly dialing into the office from poorly secured home networks. Access controls were inadequate. Endpoint devices were vulnerable. And cybercriminals were quick to exploit those weaknesses. According to the 1H Global Threat Landscape Report from FortiGuard Labs, ransomware incidents increased nearly 1100% from June 2020 to June 2021. And in a recent global ransomware survey conducted by Fortinet, an astonishing 67% of organizations report having been a ransomware target.

Despite these concerns, most enterprises are moving ahead with a hybrid work strategy that allows employees to work at least part of the time remotely. Workers may be in the office a few days a week and working from home or remotely for the rest. These workers and their devices need to move seamlessly between those environments. They need to do this while accessing applications sitting in the cloud, data center, or SaaS environments.

To make this possible, however, enterprises must also take a "work-from-anywhere" approach to their security. They need to deploy solutions capable of following, enabling, and protecting users no matter where they are located. They need security on the endpoint (EPP/EDR) combined with Zero Trust Access and ZTNA. They need Secure SD-WAN and SASE to ensure secure connectivity. Access policy engines need to provide appropriate access based on user and device identity, location, device type, and posture to establish secure access.

The challenge most organizations face is trying to do this using a dozen or more vendors. One provides endpoint protection, another provides EDR, another does identity, and so on. There may even be different firewall vendors deployed in the data center, the branch, and on the various cloud platforms in use. Creating a cohesive and reliable solution with that many vendors is nearly impossible. Ultimately, organizations end up creating complex workarounds to get solutions to even sort of work together. And maintaining those systems takes up significant amounts of IT overhead.

Fortinet Delivers Security Built for Work-from-Anywhere

That's why Fortinet has announced the industry's most complete solution for today's WFA hybrid environments. By unifying Fortinet's broad portfolio of zero trust, endpoint, and network security solutions within the Fortinet Security Fabric, organizations can secure and connect work-from-anywhere. Fortinet delivers fully integrated security, services, and threat intelligence that seamlessly follow users on the road, at home, or in the office to provide enterprise-grade protection and productivity across the extended network.

Fortinet is the only vendor capable of delivering a unified solution to simplify and satisfy the demands of today's three most common WFA scenarios—the corporate office, the home office, and the mobile worker:

Office: Because organizations rely on applications to conduct business, securing access to those applications, the networks to connect to those applications, and the devices that run those applications remain an essential component of a layered defense even when working from a traditional location. Given the potential for vulnerabilities to be exploited or third parties to be compromised, Fortinet delivers an integrated combination of essential tools, including:

Endpoint Security FortiClient, FortiEDR, and FortiXDR to secure remote workers and their devices

Zero Trust Access ZTNA (FortiClient, FortiOS, FortiGate) and Identity (FortiAuthenticator, FortiToken) to control and secure access to applications and other resources

Network Security (FortiGate and FortiGate-VM security platforms) to provide advanced and consistent security at campus, data center, branch, and cloud environments.

Work-from-Home: Remote and hybrid employees typically log in from a home office environment with a laptop, monitor, and external webcam. However, those home networks are often poorly secured with retail wireless routers and contain vulnerable IoT devices, which can be a pathway for hacker to gain access. Home networks also face challenges when it comes to supporting video conferences along with family members or roommates who might be consuming bandwidth with video streaming or online gaming activities. Fortinet delivers an integrated combination of managed, enterprise-grade security to home users, including:

Endpoint Security (FortiClient, FortiEDR, FortiXDR)

Zero Trust Access ZTNA (FortiClient, FortiOS, FortiGate) and Identity (FortiAuthenticator, FortiToken)

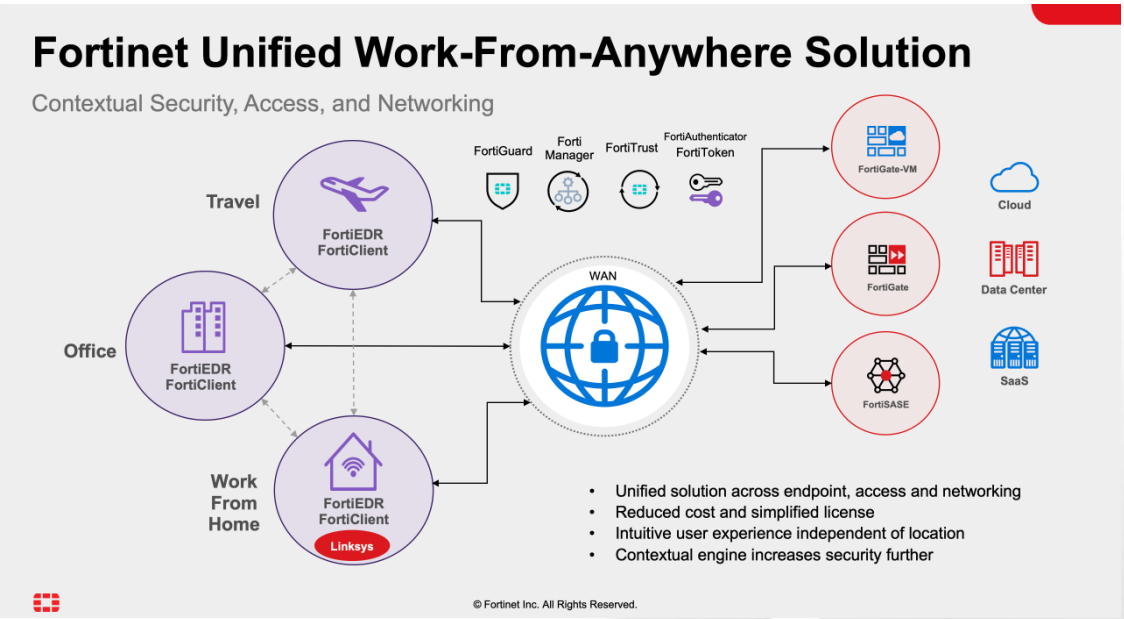
Network Security The new Linksys HomeWRK for Business | Secured by Fortinet extends FortiGate security into the home, isolates the home office, and ensures secure access to the corporate network as well as applications in the cloud and data center

Travel: Mobile workers rely on untrusted and unsecured networks to access critical business resources. This can introduce unique threats, enabling cybercriminals to intercept exposed communications or launch attacks against inadequately protected devices. To secure users on the go, Fortinet delivers an integrated combination of:

Endpoint Security FortiClient, FortiEDR, FortiXDR

Zero Trust Access ZTNA (FortiClient, FortiOS, FortiGate) and Identity (FortiAuthenticator, FortiToken)

Network Security FortiSASE Remote



Fortinet Unified Work-From-Anywhere Solution

WFA Security—Enhanced With AI/ML-driven Threat Intelligence

FortiGuard Labs leverages leading-edge AI and machine learning technologies to provide organizations with critical protection and actionable threat intelligence. These proprietary systems keep Fortinet security products armed with the best threat identification and protection information available by continuously monitoring the global attack surface using millions of network sensors and hundreds of intelligence-sharing partners.

Simplified Licensing to Support a Dynamic Workforce

Technology is only part of the solution. Fortinet is dedicated to expanding its FortiTrust security as a service portfolio, which offers simplified consumption and unified licensing models that can seamlessly follow users across any environment or form factor. FortiTrust empowers organizations to dynamically adapt to WFA challenges, such as shifting connectivity needs, hybrid workers, or resources that may need to move back and forth between physical and virtual environments and form factors without the need to adjust licensing schemes, enabling true network flexibility.

All Part of the Fortinet Security Fabric

All of this is available today as part of the Fortinet Security Fabric. Fortinet is the only vendor to support ZTNA across travel, office, and work-from-home, and the only vendor capable of delivering all the required components to support the three use cases of work-from-anywhere as part of an integrated and automated cybersecurity platform.

Source: https://www.fortinet.com/blog/business-and-technology/work-from-anywhere

6. How to Deal With Unpatched Software Vulnerabilities Right Now

According to the 2021 X-Force Threat Intelligence Index, scanning for and exploiting vulnerabilities was the top infection vector of 2020. Up to one in three data breaches stemmed from unpatched software vulnerabilities. Take a look at this list of vulnerabilities or design flaws with no official Microsoft fix. In any case, one in three might be a low-ball estimate given the increase in unpatched vulnerability attacks. How do defenders stop them?

Attacks have become more diverse over time. For example, some Linux vulnerability attackers don't want your trade secrets. Instead, they hijack computing resources for cryptomining, which can go on for months before detection. Meanwhile, threat actors can

also set up web shells to install ransomware. By maintaining the shell, they can sell remote access to your web server.

The Cybersecurity and Infrastructure Security Agency (CISA) beats the drum about software vulnerabilities and exploits. CISA says, "Foreign cyber actors continue to exploit publicly known — and often dated — software vulnerabilities against broad target sets, including public and private sector organizations. Exploitation of these vulnerabilities often requires fewer resources as compared with zero-day exploits for which no patches are available."

In other words, CISA is tired of having to deal with unpatched vulnerability breaches. Some say the lack of patching is due to laziness and neglect. Maybe it's because security teams don't have a solid patching plan. So let's hatch a plan.

Prioritize the Risk

If you were to scan your systems for software vulnerabilities, you might discover hundreds of thousands of open doors. Merged with or acquired a company recently? You just multiplied your risk. For enterprises, the grand total of detected vulnerabilities can number in the millions.

Of course, you can't patch everything at once. Instead, proper triage is essential. For example, what types of vulnerabilities are nearest to mission-critical systems?

Another factor: you can't handle this without qualified patchers. Plus, how do you know if a detected vulnerability isn't a false positive?

Common Software Vulnerabilities and Exposures

Why not target the CISA Top 10 Routinely Exploited Vulnerabilities? While it's important to be aware of the CVE list, your high-value assets may be exposed to uncommon risk. Also, CISA's Common Vulnerability Scoring System doesn't consider weaponized software vulnerabilities , that is, the ones being actively exploited. You need to consider both asset value and weaponization to triage patches.

To minimize false positives, it's important to use attack correlation, intelligence sources and a risk-based approach. This is not a simple task, and few companies have the right in-house resources. For this reason, some may choose to hire an expert team.

So Little Time, So Many Software Vulnerabilities

For vulnerability patching, the emergency room triage example serves us well. When the ER is full, doctors must decide which patients are critical. Later in the day, the ER may be nearly empty, so the doctor can address less urgent cases. Vulnerability assessment and remediation are similar. And just like the ER never closes, a company needs to audit, monitor and test their software vulnerability profile often.

Remember, your teams might add applications at any moment. So, maintain an up-to-date network inventory and schedule vulnerability scanning. Automated software vulnerability management programs can be a great help here.

Many companies don't have the time or qualified resources to identify, prioritize and remediate vulnerabilities. Rather than being lazy or negligent, businesses simply find the process overwhelming. Given the high risk involved, many companies decide to contract expert vulnerability mitigation services.

Software Patch Testing

Once your team has identified a software vulnerability, it's time to test the patch. Perhaps something worse than non-security broke an application due to a botched patch. After patch download, test each patch in a non-production environment.

Remember, with infrastructure becoming more complex, it can be difficult to test a patch in many cases. Some use cloud services as a cost-effective way to create a patch testing environment that mimics your production system.

Software Patch Bundling

Work in bundles when you can. Put another way, test and roll out patches in groups instead of one at a time. Be aware that this tactic carries some risk since an attacker may discover a vulnerability before you apply the patch. For mission-critical assets, bundling may not be the best choice. Still, in some cases, bundling leads to faster patch deployment since you're rolling out the process according to a plan.

Software Vulnerabilities: Patch Application & Verification

Since it can get confusing, IT teams should stick to a vulnerability database management schedule to keep track of patch deployment. After you apply patches, check your system logs and exceptions to verify correct patching. Also, put a recovery plan in place beforehand in case the patch causes a disaster.

To verify patch success, you can rescan your assets. This should also include checking related network devices, systems or applications for signs of malfunction.

End of Life Software & Virtual Patches

Still have outdated software or operating systems on your network? If so, threat actors can exploit existing or newly-found data protection vulnerabilities. Since old software may lack updates, the application security becomes patchless.

If legacy software sits in front of important assets, some security teams may turn to virtual patches. With virtual patches, the security enforcement layer analyzes transactions and intercepts attacks in transit. This prevents malicious traffic from reaching the web

application. While the application's actual source code stays the same, virtual patches prevent exploitation attempts.

Virtual patches are useful, scalable and much better than emergency patching. Still, virtual patching does not address all ways in which an attacker might exploit a vulnerability. For instance, a custom rule placed on a web application firewall to block access to an at-risk web page might not protect another web page that makes use of the same code.

IT teams should not rely on virtual patching as a permanent fix. Instead, it can be a bridge to more comprehensive solutions such as legacy software replacement. There's a reason CISA considers end-of-life software use as exceptionally dangerous behavior. The best thing to do is to begin planning to replace it right away. That way, it will be more likely to have patches for future software vulnerabilities, too.

Source: https://securityintelligence.com/articles/how-to-deal-with-unpatched-software-vulnerabilities-2

7. Massive Zero-Day Hole Found in Palo Alto Security Appliances

UPDATE: Researchers have a working exploit for the vulnerability (now patched), which allows for unauthenticated RCE and affects what Palo Alto clarified is an estimated 10,000 VPN/firewalls.

Researchers have developed a working exploit to gain remote code execution (RCE) via a massive vulnerability in a security appliance from Palo Alto Networks (PAN), potentially leaving 10,000 vulnerable firewalls with their goods exposed to the internet.

The critical zero day, tracked as CVE 2021-3064 and scoring a CVSS rating of 9.8 out of 10 for vulnerability severity, is in PAN's GlobalProtect firewall. It allows for unauthenticated RCE on multiple versions of PAN-OS 8.1 prior to 8.1.17, on both physical and virtual firewalls.

111021 14:04 UPDATE: The PAN updates cover versions 9.0 and 9.1, but based on Randori's research, those versions aren't vulnerable to this particular CVE. A spokesperson told Threatpost that any updates to non-8.1 versions are likely unrelated to CVE 2021-3064.

111021 17:28 UPDATE: Palo Alto has updated its advisory to clarify that this bug doesn't affect versions besides PAN-OS 8.1 prior to 8.1.17.

Randori researchers said in a Wednesday post that if an attacker successfully exploits the weakness, they can gain a shell on the targeted system, access sensitive configuration data, extract credentials and more.

After that, attackers can dance across a targeted organization, they said: "Once an attacker has control over the firewall, they will have visibility into the internal network and can proceed to move laterally."

Going by a Shodan search of internet-exposed devices, Randori initially believed that there are "more than 70,000 vulnerable instances exposed on internet-facing assets."

111021 17:30 UPDATE: Palo Alto Network informed Randori that the number of affected devices is closer to 10,000.

The Randori Attack Team found the zero day a year ago, developed a working exploit and used it against Randori customers (with authorization) over the past year. Below is the team's video of the exploit:

Don't Panic, But Do Patch

Randori has coordinated disclosure with PAN. On Wednesday, PAN published an advisory and an update to patch CVE-2021-3064.

Randori's also planning to release more technical details on Wednesday, "once the patch has had enough time to soak," and will issue updates at @RandoriAttack on Twitter, according to its writeup.

While Randori is setting aside 30 days before releasing yet more detailed technical information that it usually provides in its attack notes – a grace period for customers to patch or upgrade – it did give some higher-level details.

Vulnerability Chain Details

Randori said that CVE-2021-3064 is a buffer overflow that occurs while parsing user-supplied input into a fixed-length location on the stack. To get to the problematic code, attackers would have to use an HTTP smuggling technique, researchers explained. Otherwise, it's not reachable externally.

HTTP request smuggling is a technique for interfering with the way a web site processes sequences of HTTP requests that are received from one or more users.

These kinds of vulnerabilities are often critical, as they allow an attacker to bypass security controls, gain unauthorized access to sensitive data and directly compromise other application users. A recent example was a bug that cropped up in February in Node.js, an open-source, cross-platform JavaScript runtime environment for developing server-side and networking applications that's used in IBM Planning Analytics.

Exploitation of the buffer overflow done in conjunction with HTTP smuggling together yields RCE under the privileges of the affected component on the firewall device, according to Randori's analysis. The HTTP smuggling wasn't given a CVE identifier, as Palo Alto Networks doesn't consider it a security boundary, they explained.

To exploit the bug, an attacker needs network access to the device on the GlobalProtect service port (default port 443).

"As the affected product is a VPN portal, this port is often accessible over the Internet," researchers pointed out.

Virtual firewalls are particularly vulnerable, given that they lack Address Space Layout Randomization (ASLR), the researchers said. "On devices with ASLR enabled (which appears to be the case in most hardware devices), exploitation is difficult but possible. On virtualized devices (VM-series firewalls), exploitation is significantly easier due to lack of ASLR and Randori expects public exploits will surface." When it comes to certain hard device versions with MIPS-based management plane CPUs, Randori researchers haven't exploited the buffer overflow to achieve controlled code execution, they said, "due to their big endian architecture." But they noted that "the overflow is reachable on these devices and can be exploited to limit availability of services."

They referred to PAN's VM-Series of virtualized firewalls, deployed in public and private cloud computing environments and powered by VMware, Cisco, Citrix, KVM, OpenStack, Amazon Web Services, Microsoft and Google as perimeter gateways, IPSec VPN termination points and segmentation gateways. PAN describes the firewalls as being designed to prevent threats from moving from workload to workload.

Randori said that the bug affects firewalls running the 8.1 series of PAN-OS with GlobalProtect enabled (specifically, as noted above, versions < 8.1.17). The company's red-team researchers have proved exploitation of the vulnerability chain and attained RCE on both physical and virtual firewall products.

There's no public exploit code available – yet – and there are both PAN's patch and threat prevention signatures available to block exploitation, Randori said.

Exploit Code Sure to Follow

Randori noted that public exploit code will likely surface, given what tasty targets VPN devices are for malicious actors.

Randori CTO David "moose" Wolpoff has written for Threatpost, explaining why he loves breaking into security appliances and VPNs: After all, they present one convenient lock for attackers to pick, and then presto, they can invade an enterprise.

The Colonial Pipeline ransomware attack is a case in point, Wolpoff recently wrote: As Colonial's CEO told a Senate committee in June (PDF), attackers were able to compromise the company through a legacy VPN account.

"The account lacked multi-factor authentication (MFA) and wasn't in active use within the business," Wolpoff noted. It's "a scenario unlikely to be unique to the fuel pipeline," he added.

How Palo Alto Customers Can Mitigate the Threat

Patching as soon as possible is of course the top recommendation, but Randori offered these mitigation options if that's not doable:

- Enable signatures for Unique Threat IDs 91820 and 91855 on traffic destined for GlobalProtect portal and gateway interfaces to block attacks against this vulnerability.

- If you don't use the GlobalProtect VPN portion of the Palo Alto firewall, disable it.

For any internet-facing application:

- Disable or remove any unused features

- Restrict origin IPs allowed to connect to services

- Apply layered controls (such as WAF, firewall, access controls, segmentation)

- Monitor logs and alerts from the device

The 'Bigger Story': Ethically Using a Zero Day

Randori pointed out that Wolpoff has blogged about why zero-days are essential to security, and the Palo Alto Networks zero day is a prime example.

"As the threat from zero-days grows, more and more organizations are asking for realistic ways to prepare for and train against unknown threats, which translates to a need for ethical use of zero-days," the researchers said in their writeup. "When a defender is unable to patch a flaw, they must rely on other controls. Real exploits let them validate those controls, and not simply in a contrived manner. Real exploits let customers scrimmage against the same class of threats they are already facing."

Source: https://threatpost.com/massive-zero-day-hole-found-in-palo-alto-security-appliances/176170/

8. How to Live a Digital Life Free of Spyware

Spyware is tricky. Some types notify users that they're monitoring activity. Others function in stealth mode and use the information they collect for nefarious purposes. Spyware is a type of software that collects data about online users and reports it to a company or an individual. What just about everyone can agree on is that anonymous browsing is looking more and more appealing and is likely the way of the future.

Here's more about the types of spyware, which types are legal, and how you can scrub your device and live more confidently online.

Types of Spyware

Here are a few types of spyware and facts about each:

Keyloggers

Is it legal? Definitely not!

What is its purpose? Criminal

Keyloggers are the most intrusive of the spyware variations. It does exactly as its name suggests: It takes note of keyboard strokes, logs them, and reports to the owner of the nefarious software. Once the cybercriminal has digitally looked over your shoulder at your online activity, they make note of your passwords, walk into your online accounts, and pilfer your private personal information. They could use this information to gain entry to your online bank accounts or steal your identity.

Keyloggers are downloaded onto devices (cellphones, tablets, laptops, or desktop computers) without the user's knowledge. Cybercriminals can hide them within email attachments or in malicious web pages. So, the best way to steer clear of keyloggers is to never download attachments you're unsure about and don't visit sites that seem unprofessional. One rule of thumb is to mostly stick to URLs that begin with https and include a lock icon. These sites are almost always secure.

To determine if your device is infected with a keylogger, check your system's performance. Is your device running slowly? See if there are any spikes in activity or unknown programs running in the background. This could indicate that your device is hosting a malicious program.

Adware

Is it legal? Sometimes

What is its purpose? Advertising and criminal

Adware is categorized as a type of spyware. It tracks users' online activity and spits out targeted pop-up advertisements. If you have the pop-up blocker enabled on your browser, you'll likely be spared from the annoyance. Additionally, pop-ups can slow your device, so that's another reason to turn on the pop-up blocking feature. Legitimate adware often asks users to opt into targeted ads.

Adware turns malicious (and illegal) when it contains malware. Sometimes cyber criminals hide malware within pop-ups. It's easy to accidentally hit a link within a pop-up when you're aiming quickly for the X to close it.

It's easy to spot a device with an adware infestation. First, the number of pop-ups will be out of control. Also, the device will crash often, run very slowly, and have a short battery life. An antivirus program will likely be able to identify and remove the culprit. You can also check out your system monitor and end tasks that are draining your device's power.

Cookies

Is it legal? Yes

What is its purpose? Advertising

Cookies are delicious, especially to advertisers who use them to better target ads and make profits selling collected user data to third-party companies. Cookies are sometimes categorized as spyware, because they log the websites you visit and report them. You may notice the banners on websites that ask you to accept cookies.

Many users today are uneasy with sharing their online activity with strangers and advertisers. Sometimes the ads that pop up on your social media feed or in sidebars seem a little too targeted and it feels like someone is listening in to your conversations and attempting to make a profit from them.

How to Browse Free of Spyware

To scrub cybercriminals from your devices and confuse advertisers, consider the following steps you can easily add to your daily routine:

Clear your cache periodically. This is a quick way to delete all the cookies from your device. It also helps if your device is running slowly. Clearing your cache deletes your browsing history, meaning that you won't be able to type in your usual shortcuts to your most-visited sites and the browser won't automatically auto-fill the rest of the URL or remember your passwords. Consider making bookmarks of your favorite sites for quick access and entrust your passwords to a password manager that will remember them for you.

Know how to spot phishing attempts. Cybercriminals often hide their spyware within phishing texts and emails, so it's key to know how to spot them. Phishers trick users into acting quickly, either through scare tactics or fake exciting news, to download attachments or give up personal information. Luckily, phishing attempts usually aren't too difficult to identify and delete immediately. Did you enter a contest lately? No? Then why would someone get in touch saying you're a winner? Also, phishing messages are often full of typos and poor grammar. Before you click any links in an email, hover your cursor over it to see where the URL will take you. If it has typos, is filled with a long string of letters or numbers, or doesn't match the site the message says it'll redirect you to, delete it.

Browse in incognito mode. Browser sallow users to toggle incognito mode to use the internet anonymously. Once users exit incognito mode, all of their browsing history and the cookies collected during the session are deleted. Incognito mode, though effective against cookies, does not combat keyloggers or aggressive adware.

Use a VPN. A virtual private network (VPN) is even more secure than incognito mode. It completely scrambles your online data, making it impossible for a spy to hack into your device if you're connected to a public wi-fi network. A VPN doesn't stop cookies, but the geographic information they report may be incorrect.

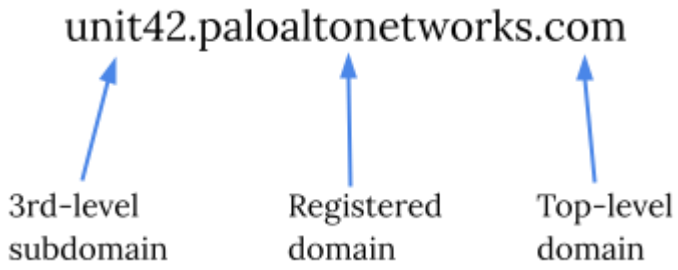
Sign up for antivirus software. A comprehensive online protection software suite that includes antivirus software, such as McAfee Total Protection, can boost your confidence in your online safety. It can scan your phone, tablet, or computer for viruses or malware and automatically logs you into a VPN for secure browsing.

Source: https://www.mcafee.com/blogs/consumer-cyber-awareness/how-to-live-a-digital-life-free-of-spyware/

9. These are the top-level domains threat actors like the most

Out of over a thousand top-level domain choices, cyber-criminals and threat actors prefer a small set of 25, which accounts for 90% of all malicious sites.

Six out of the top 10 of these 25 top-level domains (TLD) are handled by authorities in developing countries, hosting a disproportionately large number of risky sites compared to their populations.



Example of a TLD
Source: Unit42

These stats are revealed in an in-depth analysis from researchers at Palo Alto Networks, who took a deep dive into the TLDs commonly used by threat actors and why they are being chosen.

The categories picked for analysis are malware, phishing, command and control (C2), and grayware (adware, 'joke malware,' spyware).

The worst cases

Using data collected on October 7th, 2020, Palo Alto Networks analyzed domains categorized by their Advanced URL Filtering service, and that met specific criteria.

"First, we only study domains categorized by the Advanced URL Filtering service, and we only consider registered domains (also called root domains). Additionally, we validate whether domains existed the past one year by checking zone files and passive DNS, and by issuing active DNS queries. We do not consider domains that we categorize as parked, insufficient content or unknown for our calculations," explains the research by Palo Alto Networks Unit42.

"Further, when calculating reputation scores, we don't consider domains sinkholed for preemptive measures as malicious. Finally, we only consider TLDs with at least a hundred domains, as smaller TLDs likely have policies in place restricting entities allowed to register domain names. This blog post is based on data collected on Oct. 7, 2021."

Using this data, Palo Alto Networks created the following summary table to give an overview of the malicious use of the top TLDs for each category and their cumulative distribution (CD). The higher the CD, the more that particular TLD is used for the category.

Total		Malicious		Phishing		Malware		Grayware		C2		Sensitive	
TLD	CD	TLD	CD	TLD	CD	TLD	CD	TLD	CD	TLD	CD	TLD	CD
com	0.47	com	0.49	com	0.41	com	0.51	xyz	0.38	com	0.58	com	0.39
net	0.51	icu	0.53	xyz	0.48	icu	0.56	com	0.68	net	0.66	tk	0.48
de	0.55	xyz	0.58	tk	0.52	cn	0.61	tokyo	0.71	tk	0.72	icu	0.54
org	0.58	cn	0.62	ml	0.55	net	0.66	club	0.73	cn	0.76	ga	0.59
tk	0.61	net	0.66	cf	0.59	ml	0.70	net	0.75	info	0.79	cf	0.63
uk	0.63	ml	0.70	icu	0.61	org	0.72	work	0.76	cf	0.82	gq	0.67
cn	0.65	tk	0.73	ga	0.64	tk	0.75	ru	0.77	ml	0.85	ml	0.71
ru	0.67	org	0.75	top	0.66	cf	0.77	co	0.79	ga	0.88	cn	0.74
icu	0.68	cf	0.77	pw	0.68	xyz	0.79	info	0.80	gq	0.91	xyz	0.77
xyz	0.70	ga	0.79	net	0.70	ga	0.80	org	0.81	top	0.92	net	0.80

Table 1: TLDs with the highest volumes of malicious content distribution
Source: Unit42

The most popular top-level domain is .com, which has an average ratio of malicious domains. Crooks tend to use it because it adds legitimacy and generally improves their success rates.

Those that fair the worse in the 'cumulative distribution' category are .xyz, .icu, .ru, .cn, .uk, and tk. This means that most of the bad stuff circulating the web in terms of volume comes from these domains.

The TLDs that distribute malware the most are .ga, .xyz, .cf, ,tk, .org, and .ml.

Phishing actors prefer to use .net domains, with .pw, .top, .ga, and .icu, following with notable volumes. However, the researchers found phishing to be one of the most evenly distributed categories, with 99% of the domains spreading across 92 different TLDs.

Grayware is being distributed through .org, .info, .co, .ru, .work, .net, and .club domains, indicative of the trickery that underpins this category of software.

Finally, C2 infrastructure usually relies on .top, .gq, .ga, .ml, .cf, .info, .cn, and .tk.

Palo Alto compiled the following table in terms of the rate of malicious domains compared to the total registrations for a TLD.

In the table below, the MAD score is the 'median of the absolute deviation,' which means that a higher score represents an unusually large number of malicious domain registrations for that TLD.

Malicious		Phishing		Malware		Grayware		C2	
TLD	MAD	TLD	MAD	TLD	MAD	TLD	MAD	TLD	MAD
zw	30.37	pw	43.48	zw	38.05	sbs	89.66	cyou	7.95
bd	26.18	quest	32.00	bd	30.98	tokyo	66.08	pw	6.72
ke	25.38	ke	17.28	ke	28.69	xyz	40.94	ws	4.25
am	18.48	date	15.47	am	24.46	cam	21.21	gq	4.03
sbs	17.58	cyou	13.80	cd	16.07	date	18.56	cf	3.84
date	15.38	support	11.38	date	13.12	cm	16.21	ml	3.81
pw	13.35	win	8.55	bid	12.81	casa	15.78	ga	3.36
quest	11.92	rest	7.14	ml	12.00	uno	11.77	info	2.93
cd	11.88	casa	6.45	ws	10.68	email	8.39	su	2.74
bid	10.96	help	5.47	icu	9.08	stream	7.38	best	2.44

TLDs with the highest rate of malicious domains
Source: Unit42

Why does any of that matter?

The fact that the TLD domains for Tokelau, a small island in the Pacific, are in the top ten of all malicious categories means that the relevant registration authority is likely not following strict reviewing practices.

"One of the most fascinating stories in the domain name world is how .tk, the ccTLD of a small Pacific island called Tokelau, became one of the most populous TLDs in the world. Domain registrations contributed at one point one-sixth of Tokelau's income," explains the report by Palo Alto Networks.

"Their TLD became popular by providing free domain registrations, where the source of income for the TLD operator is through advertisement rather than domain registration fees. Unfortunately, their domain registration policy also invites abuse, spam and a large amount of sensitive content, as we can observe in Table 1."

The same applies to .pw and .ws domains, controlled by the Republic of Palau and Western Samoa.

These countries offer cheap or even free domain registrations to generate income from ads running on sites.

This advertising model generates significant revenue from domain registrations but also opens the door for widescale abuse.

This, of course, doesn't mean that large TLDs such as .net, .org, and .xyz, can afford to relax against abusive registrations. On the contrary, the stats show that popular TLDs are more responsible for clearing up malicious registrations.

In many cases, legitimate domains on these larger TLDs are compromised by threat actors, so they were not registered with malicious intent.

Another reason why such reports are helpful is that they can help Internet security solutions strengthen their malicious domain detection algorithms.

These rates can be used as factors that are evaluated in conjunction with other elements to generate a total risk score when determining if security software or gateways should block an URL.

Source: https://www.bleepingcomputer.com/news/security/these-are-the-top-level-domains-threat-actors-like-the-most/

10. Penetration Testing for Cloud-Based Apps: A Step-by-Step Guide

Although cloud providers offer more and more robust security controls, in the end, you're the one who has to secure your company's workloads in the cloud. According to the 2019 Cloud Security Report, the top cloud security challenges are data loss and data privacy, followed by compliance concerns, tied with worries about accidental exposure of credentials. Cloud penetration testing can help with this.

What is cloud pen testing? It is an authorized simulation of a cyberattack against a system that is hosted on a cloud provider, e.g., Google Cloud Platform, Microsoft Azure, Amazon Web Services (AWS), etc. Its main objective is to find the threats and weaknesses of a system hosted on a cloud platform so that you can see how secure it really is. Cloud app pen testing also requires a shared responsibility model.

Shared Responsibility in Cloud Penetration Testing

In a cloud computing environment, there are two terms with which you need to be familiar:

Provider: Provider is the entity that builds and runs the cloud environment and offers its services on a metered basis to one or more tenants.

Tenant: Tenant is the entity that is using the metered service of the cloud provider.

When determining the scope, you should check whether the organization is a cloud provider or tenant. For multiple clouds, an organization can act as a provider for one and a tenant for others.

Cloud Service Models

Before penetration testing cloud-based applications, you should understand which resources the cloud service provider will take care of and which resources the tenant will take care of.

Infrastructure-as-a-Service (IaaS): Hardware and network connectivity are supplied by the cloud provider. The tenant takes care of the virtual machine and everything that runs within it.

Platform-as-a-Service (PaaS): The provider supplies all the components required to run the application, and the tenant supplies the application it wishes to deploy.

Cloud penetration testing works in PaaS and IaaS environments as long as you work together with the cloud service provider. Note that there is a third option: Software-as-a-Service (SaaS). In this case, the provider supplies the application and all the components required to run it. Due to the impact on the infrastructure, providers don't allow penetration testing in the SaaS environment.

Understand the Policies of the Cloud Service Provider

Putting aside private clouds, public clouds have policies related to security testing. You need to notify the provider that you are going to carry out penetration testing and comply with the restrictions on what you can actually perform during the testing.

Many public cloud providers have a certain process that needs to be followed. Not adhering to the process could get you in legal trouble. For example, if your testing leads to a distributed denial-of-service (DDoS) attack, the provider may shut down your account.

Public clouds are multi-tenant. Your penetration testing could also take up so many resources that it affects other tenants in the cloud. There are rules for this, so you need to understand the legal requirements, policies and procedures before carrying it out.

Create a Penetration Testing Plan

A penetration testing strategy for a cloud-based app should include the following:

User interfaces: Identify and include user interfaces in the specific application

Network access: Examine how well the network safeguards the application and data

Data: Check how the testers will test the data as it passes through the application and into the database

Virtualization: Determine how well virtual machines can separate your workload

Automation: Select automated tools

Regulation: Know the laws and regulations you need to adhere to within the application or database

Approach: Determine whether application admins should be included.

Select Your Penetration Testing Tools

There are a plethora of penetration testing tools on the market. While it's common to use on-premises tools to test cloud-based services, you can now also use cloud-based testing tech that may be more cost-effective. Furthermore, they do not require a large amount of hardware. The tool's main feature is that it can imitate an actual attack.

Observe the Response

Look for the following things while performing the penetration testing:

The human response, or how the application's admins and users react to it. The responses will be more telling if you don't make the test public. Many people will just shut down the system, while others may diagnose the problem first before detecting and escalating the threat. This includes your cloud provider's people; how they respond is just as crucial.

The security system's automated response, or how it can detect and respond to penetration testing. Make sure that reaction is multi-tiered, with options ranging from merely banning the IP address that generated the test to shutting down the system. In any case, notify security and application administrators, and supply them with the details of the corrective action performed.

It's important to keep track of both human and automated responses. This is where you'll uncover any flaws in the systems and people's responses to the danger, as well as the system's overall defenses.

Find and Remove Vulnerabilities

While this may seem like an obvious step, in the end, you'll have a list of vulnerabilities identified by penetration testing. The list could be hundreds of issues long or as short as two or three.

If there aren't any, your testing may not be as effective as it should be, and you should consider it again and retry.

Vulnerabilities discovered during penetration testing of cloud-based apps often look like this:

- Using an application programming interface (API), you can access application data
- After 10 failed tries, the tester gained API access
- The virtual machine does not isolate the workload well enough
- The tester guessed the password for the application using an automated password generator
- If the tester turns off DNS, a virtual private network allows access from the outside
- Encryption does not meet new regulations
- Other issues.

Of course, the issues you discover will differ based on the application and type of penetration testing you conduct. Also, keep in mind that there are other layers to consider.

Perform separate tests on the application, network, database and storage layers, and report issues one by one. The layers should also be tested jointly to study how well they work together and if there are any concerns. It's best practice to report what happened at each layer as a whole.

Final Pen Testing Suggestions

Another factor to examine is who is conducting the penetration testing. If you handle it in-house, you can be sure that some difficulties will go unnoticed. Internal testing teams, no matter how skilled they are, can overlook something. They're too near to the action and too familiar with the software, which can lead to carelessness and errors.

You should consider best practices for your cloud provider, the applications you'll be testing and any compliance requirements you'll need to meet. Using the methods that others have used is a fantastic place to start, but keep in mind that you should tailor your penetration testing methods and tools to your specific needs.

Penetration testing is no longer optional. It's the only method to demonstrate that your cloud-based services and data are safe enough to allow a large number of users to access them with minimal risk.

Source: https://securityintelligence.com/posts/penetration-testing-cloud-apps-guide/

11. Common Cloud Misconfigurations Exploited in Minutes, Report

Opportunistic attackers instantly exploited insecurely exposed services deployed in honeypots by Unit 42 researchers, demonstrating the immediate danger of these typical mistakes.

Poorly configured cloud services can be exploit by threat actors in minutes and sometimes in under 30 seconds. Attacks include network intrusion, data theft and ransomware infections, researchers have found.

Researchers at Palo Alto Networks' Unit 42 used a honeypot infrastructure of 320 nodes deployed globally in which they misconfigured key services within a cloud–including remote desktop protocol (RDP), secure shell protocol (SSH), server message block (Samba) and Postgres database.

What they found was that attackers jumped at the opportunity to exploit the misconfigurations, with 80 percent of the 320 honeypots compromised within 24 hours and all compromised within a week, researchers disclosed in a report posted Monday.

Moreover, some attacks occurred within minutes, with one particularly speedy threat actor compromising 96 percent of the 80 honeypots globally within 30 seconds, researchers found.

Given that the speed with which organizations typically manage vulnerabilities is typically measured in days or months, "that fact that attackers could find and compromise our honeypots in minutes was shocking," Unit 42 principal cloud security researcher Jay Chen wrote in the post.

Common Cloud Mistakes

The study clearly shows how quickly these common misconfigurations can lead to data breaches or attackers' taking down an entire network—given that "most of these internet-facing services are connected to some other cloud workloads," Chen wrote. This reinforces the importance of mitigating and patching security issues quickly, he said.

"When a misconfigured or vulnerable service is exposed to the internet, it takes attackers just a few minutes to discover and compromise the service," Chen wrote. "There is no margin of error when it comes to the timing of security fixes."

Indeed, scores of high-profile cyber incidents have occurred because of misconfigured cloud services. This year alone two popular commercial outlets—the Hobby Lobby retail chain and Wegman's grocery stores—experienced separate data breaches due to these types of mistakes.

Hobby Lobby exposed customer data because of a cloud-bucket misconfiguration, while Wegman's also leaked customer data because two of its cloud-based databases were misconfigured.

Luring Attackers

Unit 42 conducted the current cloud-misconfiguration study between July 2021 and August 2021, deploying 320 honeypots with even distributions of SSH, Samba, Postgres and RDP across four regions–North America (NA), Asia Pacific (APAC) and Europe (EU). Their research analyzed the time, frequency and origins of the attacks observed during that time in the infrastructure.

To lure attackers, researchers intentionally configured a few accounts with weak credentials such as admin:admin, guest:guest, administrator:password, which granted limited access to the application in a sandboxed environment. They reset honeypots after a compromising event—i.e., when a threat actor successfully authenticated via one of the credentials and gained access to the application.

Researchers also blocked a list of known scanner IPs on a subset of honeypots, updating firewall policies once a day based on the observed network scanning traffic.

The team analyzed attacks according to a variety of attack patterns, including: the time attackers took to discover and compromise a new service; the average time between two consecutive compromising events of a targeted application; the number of attacker IPs observed on a honeypot; and the number of days an attacker IP was observed.

Specific Results

Results of the study showed that the Samba honeypots were the ones attacked most quickly, as well as the ones with attackers that compromised the services most consecutively with the most speed.

However, SSH was the misconfigured service with the highest number of attackers, experiencing a number of attackers and compromising events that was much higher than for the other three applications, researchers reported. The most attacked SSH honeypot was compromised 169 times in a single day, while on average, each SSH honey suffered 26 attacks daily, they found.

Researchers also tracked attacks according to region, with Samba and RDP getting the most attacks from North America, while attacks from APAC targeting Postgres and SSH more frequently, they found.

Overall, 85 percent of the attacks on the honeypots were observed on a single day, which indicated to researchers that blocking known scanner IPs is ineffective in mitigating attacks, as attackers rarely reuse the same IPs to launch attacks, Chen wrote.

Avoiding Common Cloud Mistakes

The good news for organizations making common cloud configuration mistakes that can be easily exploited is that they also are easy to avoid, researchers said. Chen listed several recommendations for system administrators to avoid leaving services exposed to attacks.

To safeguard services from being pummeled by attacker IPs, cloud administrators can implement a guardrail to prevent privileged ports from being open, as well as create audit rules to monitor all the open ports and exposed services.

Researchers also suggested that admins create automated response and remediation rules to fix misconfigurations automatically and deploy next-generation firewalls to block malicious traffic.

Source: https://threatpost.com/cloud-misconfigurations-exploited-in-minutes/176539/

12. UK government transport website caught showing porn

A UK Department for Transport (DfT) website was caught serving porn earlier today.

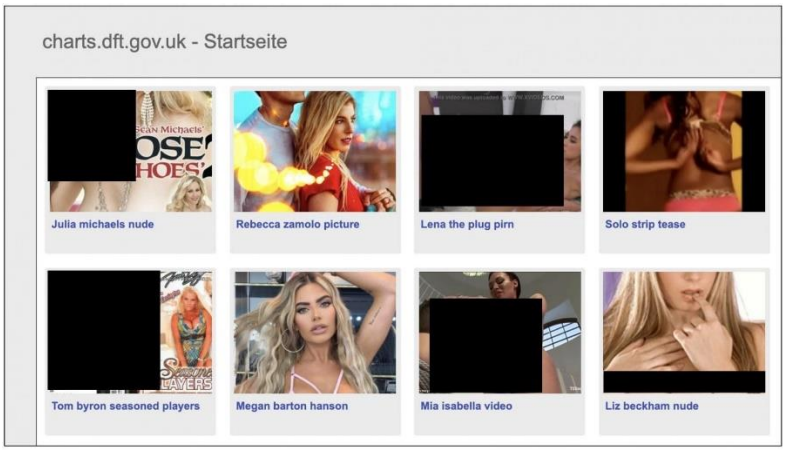
The particular DfT subdomain behind the mishap, on most days, provides vital DfT statistics for the public and the department's business plan.

Racy traffic ahead

The UK DfT's charts.dft.gov.uk website was seen serving porn today, as confirmed by BleepingComputer.

In the past, the Charts subdomain has provided business plan documents and important statistics on various DfT services such as numbers on public transport utilization, roadway accessibility times, and driving tests.

Although the site is no longer reachable, as of a few hours ago, visiting charts.dft.gov.uk paved the way for some racy traffic:



UK gov DfT subdomain caught serving porn (BleepingComputer)

The mishap was first spotted by The Crow, which additionally observed that the entire dft.gov.uk domain was itself made to redirect to a WordPress plugin page, while the Department appeared to investigate the issue.

In our tests, BleepingComputer observed the official dft.gov.uk website led to a password-protected WordPress page living at: eu-hauliers.dft.gov.uk.

The entire dft.gov.uk redirected to a password-protected WordPress page earlier today (BleepingComputer)

The dangling... DNS

Although the exact cause of the Charts mini-site serving porn is not known, it appears the subdomain did have a CNAME DNS record pointing to an Amazon S3 instance.

The offending (NSFW) instance is still up at charts.dft.gov.uk.s3-website-eu-west-1.amazonaws.com, showing illicit content. Fortunately, charts.dft.gov.uk no longer leads there.

What remains unclear is, if this was simply a case of domain hijacking—that is, a dangling AWS S3 instance that the Charts site pointed to, was claimed by a threat actor and made

to serve adult content, or did an attacker obtain enough access to DfT's registrar's systems and changed the DNS entry for charts.dft.gov.uk.

The second scenario is more challenging to pull off and would raise some serious questions on how secure the DfT's digital infrastructure is.

"A disused, dormant page of the Department for Transport's Gov.uk website has been used," a DfT spokesperson told BleepingComputer.

"No information or data has been lost or compromised. The website address has since been permanently deleted."

This isn't the first time a government website was caught serving explicit content either.

In September this year, U.S. government websites were spammed with viagra ads and adult content after attackers exploited a vulnerability in the Laserfiche Forms software product, used by multiple government sites.

In July, visitors to major news sites including The Washington Post and HuffPost saw the embedded videos in news stories replaced with porn after the vid.me domain was acquired by a third party.

The access to the main DfT website dft.gov.uk has since been restored. But, as stated, the sysadmins have pulled the plug on charts.dft.gov.uk altogether, which is no longer accessible.

Source: https://www.bleepingcomputer.com/news/security/uk-government-transport-website-caught-showing-porn/

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.