



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

Monthly Security Bulletin

February 2021

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.	Ransomware and DDoS is on the Rise: Tips for Distance Learning in 2021	4
2.	Telegram feature exposes your precise address to hackers	7
3.	Hackers leaked altered Pfizer data to sabotage trust in vaccines	9
4.	Privacy-focused search engine DuckDuckGo grew by 62% in 2020	10
5.	Malwarebytes says SolarWinds hackers accessed its internal emails	12
6.	Space Cybersecurity: How Lessons Learned on Earth Apply in Orbit.....	13
7.	Here's how a researcher broke into Microsoft VS Code's GitHub.....	18
8.	Here's how law enforcement's Emotet malware module works	21
9.	Fonix ransomware shuts down and releases master decryption key	24
10.	Data of 66,000 users left open on a misconfigured Elasticsearch server	27
11.	Microsoft Edge, Google Chrome Roll Out Password Protection Tools.....	29

1. Ransomware and DDoS is on the Rise: Tips for Distance Learning in 2021

The holidays have come and gone, and students returned to the virtual classroom. But according to the FBI, cyberattacks are likely to [disrupt online learning](#) in the new year. As of December 2020, the FBI, Cybersecurity and Infrastructure Security Agency (CISA), and MS-ISAC continue to receive reports from K-12 educational institutions about the disruptions caused by cyberthreats, primarily ransomware and Distributed Denial of Service (DDoS). To protect their education and digital lives, distance learners will need to stay vigilant when it comes to ransomware and DDoS attacks. Let's dive into the impact these threats have on the K-12 education system now that more people are plugged in as a result of distance learning.

Hackers Hold Education for Ransom

Of all the attacks plaguing K-12 schools this year, ransomware has been a particularly aggressive threat. Ransomware attacks typically block access to a computer system or files until the victim pays a certain amount of money or "ransom." The FBI and the CISA issued a warning that showed a nearly 30% increase in ransomware attacks against schools. In August and September, 57% of ransomware incidents involved K-12 schools, compared to 28% of all reported ransomware incidents from January through July. And it's unlikely that hackers will let up anytime soon. [Baltimore County's school system](#) was recently shut down by a ransomware attack that hit all of its network systems and closed schools for several days for about 111,000 students. It wasn't until last week that school officials could finally regain access to files they feared were lost forever, including student transcripts, first-quarter grades, and vital records for children in special education programs.

According to [ZDNet](#), the five most active ransomware groups targeting K-12 schools are [Ryuk](#), Maze, Nefilim, AKO, and Sodinokibi/REvil. Furthermore, all five of these ransomware families are known to run "leak sites," where they dump data from victims who don't pay the ransom. This creates a particularly dangerous problem of having student data published online. To prevent distance learning disruption, students and educators need to understand the effects of ransomware on school systems and take steps to prevent the damage caused by this threat.

DDoS Attacks Disrupt the Distance Learning

An increase in ransomware attacks isn't the only problem that K-12 schools are facing. The CISA and the FBI warned those participating in distance learning to protect themselves against other forms of cyberattacks such as Distributed Denial of Service (DDoS). DDoS is a method where hackers flood a network with so much traffic that it cannot operate or communicate as it normally would.

According to [Dark Reading](#), Miami-Dade County Public Schools experienced significant disruptions during their first three days of distance learning for the 2020-2021 school year, thanks to a series of DDoS attacks. The school system stated it had already experienced more than a dozen DDoS attacks since the start of the school year. Sandwich Public Schools in Massachusetts were also knocked offline by a DDoS attack. When school systems fall victim to DDoS attacks, students can lose access to essential documents, files, or online platforms that they need to complete assignments. And with many students relying heavily on distance learning systems, losing access could put them behind.

Delete Disruptions: Follow These Security Tips

In an effort to create a standardized framework for dealing with ransomware attacks across verticals – including education – McAfee has teamed up with Microsoft to lead the [Ransomware Task Force](#), along with 17 other security firms, tech companies, and non-profits. And while we're taking critical actions to decrease the threat of ransomware attacks, there are other steps you can take to prevent ransomware and DDoS attacks from interrupting your distance learning experience. Follow these tips to take charge of your education and live your digital life free from worry:

Don't pay the ransom

Many ransom notes seem convincing, and many only request small, seemingly doable amounts of money. Nevertheless, you should never pay the ransom. Paying does not promise you'll get your information back, and many victims often don't. So, no matter how desperate you are for your files, hold off on paying up.

Do a complete backup

With ransomware attacks locking away crucial data, it's important to back up your files on all your machines. If a device becomes infected with ransomware, there's no promise you'll get that data back. Ensure you cover all your bases and have your data stored on an external hard drive or in the cloud.

Use decryption tools

[No More Ransom](#) – an initiative that teams up security firms, including McAfee, and law enforcement – provides tools to free your data, each tailored for a specific type of ransomware. If your device gets held for ransom, start by researching what type of ransomware it is. Then, check out [No More Ransom's decryption tools](#) and see if one is available for your specific strain.

Secure your router

Your Wi-Fi router is the gateway to your network. Secure it by changing the default password. If you aren't sure how to do this, consult the internet for instructions on how to do it for your specific make and model, or call the manufacturer. Solutions like McAfee Secure Home Platform, which is embedded within select routers, can help you easily manage and protect your network from DDoS attacks and more.

Change default passwords on IoT devices

A lot of internet of things (IoT) devices come with default usernames and passwords. After taking your IoT device out of the box, the first thing you should do is change those default credentials. If you're unsure of how to change the default setting on your IoT device, refer to setup instructions or do a bit of research online.

Source: <https://www.mcafee.com/blogs/consumer/consumer-threat-notice/ransomware-and-ddos-is-on-the-rise-tips-for-distance-learning-in-2021/>

2. Telegram feature exposes your precise address to hackers

If you're using an Android device—or in some cases an iPhone—the Telegram messenger app makes it easy for hackers to find your precise location when you enable a feature that allows users who are geographically close to you to connect. The researcher who discovered the disclosure vulnerability and privately reported it to Telegram developers said they have no plans to fix it.

The problem stems from a feature called People Nearby. By default, it's turned off. When users enable it, their geographic distance is shown to other people who have it turned on and are in (or are spoofing) the same geographic region. When People Nearby is used as designed, it's a useful feature with few if any privacy concerns. After all, a notification that someone is 1 kilometer or 600 meters away still leaves stalkers guessing where, precisely, you are.

Stalking made simple

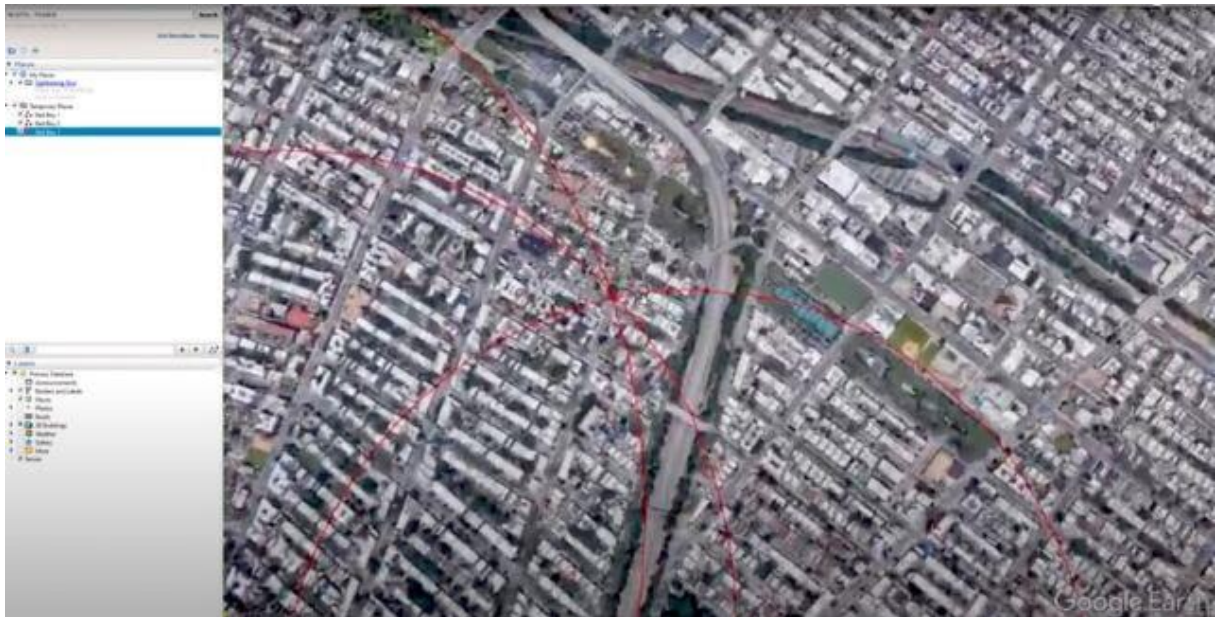
Independent researcher [Ahmed Hassan](#), however, has shown how the feature can be abused to divulge exactly where you are. Using readily available software and a rooted Android device, he's able to spoof the location his device reports to Telegram servers. By using just three different locations and measuring the corresponding distance reported by People Nearby, he is able to pinpoint a user's precise location.

Telegram lets users create local groups within a geographical area. Hassan said that scammers often spoof their location to crash such groups and then peddle fake bitcoin investments, hacking tools, stolen social security numbers, and other scams.

"Most users don't understand they are sharing their location, and perhaps their home address," Hassan wrote in an email. "If a female used that feature to chat with a local group, she can be stalked by unwanted users."

A proof-of-concept video the researcher sent to Telegram showed how he could discern the address of a People Nearby user when he used a free GPS spoofing app to make his phone report just three different locations. He then drew a circle around each of the three locations with a radius of the distance reported by Telegram. The user's precise location was where all three intersected.

Hassan asked that the video not be published. The screenshot below, however, gives the general idea.



Enlarge
Ahmed Hassan

Fixing the problem

In a [blog post](#), Hassan included an email from Telegram in response to the report he had sent them. It noted that People Nearby isn't enabled by default and that "it's expected that determining the exact location is possible under certain conditions."

Telegram representatives didn't respond to an email seeking comment.

People Nearby poses the biggest threat to people using Android devices, since they report a user's location with enough granularity to make Hassan's attack work. The recently released iOS 14, by contrast, allows users to divulge only a rough approximation of their location. People who use this feature aren't as exposed.

Fixing the problem—or at least making it much harder to exploit it—wouldn't be hard from a technical perspective. Rounding locations to the nearest mile and adding some random bits generally suffices. When the Tinder app had a similar disclosure vulnerability, developers used this kind of technique to fix it.

The privacy consequences of Telegram's People Nearby feature are a good reminder that features can often be abused in ways that aren't contemplated by the people who develop them. Users who want to keep their whereabouts private should be suspicious of location-based services and do research before installing or turning them on.

Source: <https://arstechnica.com/information-technology/2021/01/telegram-feature-exposes-your-precise-address-to-hackers/>

3. Hackers leaked altered Pfizer data to sabotage trust in vaccines

The European Medicines Agency (EMA) today revealed that some of the stolen Pfizer/BioNTech vaccine candidate data was doctored by threat actors before being leaked online with the end goal of undermining the public's trust in COVID-19 vaccines.

EMA is the decentralized agency that reviews and approves COVID-19 vaccines in the European Union, and the agency that evaluates, monitors, and supervises any new medicines introduced to the EU.

"The ongoing investigation of the cyberattack on EMA revealed that some of the unlawfully accessed documents related to COVID-19 medicines and vaccines have been leaked on the internet," the agency disclosed today.

"This included internal/confidential email correspondence dating from November, relating to evaluation processes for COVID-19 vaccines.

"Some of the correspondence has been manipulated by the perpetrators prior to publication in a way which could undermine trust in vaccines."

EMA revealed that the COVID-19 vaccine data stolen in December was leaked online in a previous update, on Tuesday.

Pointing fingers at "fake vaccines"

BleepingComputer became aware of several threat actors leaking what they claimed to be the stolen EMA data on multiple hacker forums on December 31st.

Several sources in the cybersecurity intelligence community told BleepingComputer that the leaked data archives included email screenshots, EMA peer review comments, as well as Word, PDF, PowerPoint documents.

Below is a screenshot of one of the data leaks seen by BleepingComputer at the time, linking to archives containing the altered documents stolen during the EMA attack.

As the screenshot shows, the intent of the threat actor behind the leak was to highlight that the Pfizer COVID-19 vaccine was fake, confirming EMA's disclosure that the leaked documents were manipulated with the purpose of weakening trust in the vaccines.

Following the December attack, the agency disclosed that it launched a joint investigation in collaboration with law enforcement and several other relevant entities.

Pfizer and BioNTech jointly disclosed that some COVID-19 documents relating to the regulatory submission stored on EMA's servers were accessed by the threat actors behind the cyberattack.

EMA later revealed that the investigation shows that only a limited number of documents linked to the BNT162b2 COVID-19 vaccine candidate were accessed without authorization during the incident.

EMA also discovered that the data breach was limited to a single IT app, with the threat actors behind this attack primarily targeting data related to COVID-19 vaccines and medicines.

Source: <https://www.bleepingcomputer.com/news/security/hackers-leaked-altered-pfizer-data-to-sabotage-trust-in-vaccines/>

4. Privacy-focused search engine DuckDuckGo grew by 62% in 2020

The privacy-focused search engine DuckDuckGo continues to grow rapidly as the company reached 102M daily search queries for the first time in January.

[DuckDuckGo](#) is a search engine that builds its search index using its DuckDuckBot crawler, indexing Wikipedia, and through partners like Bing. The search engine does not use any data from Google.

What makes DuckDuckGo stand out is that they do not track your searches to build a user profile or share any personal or identifying data with third-party companies, including ad networks.

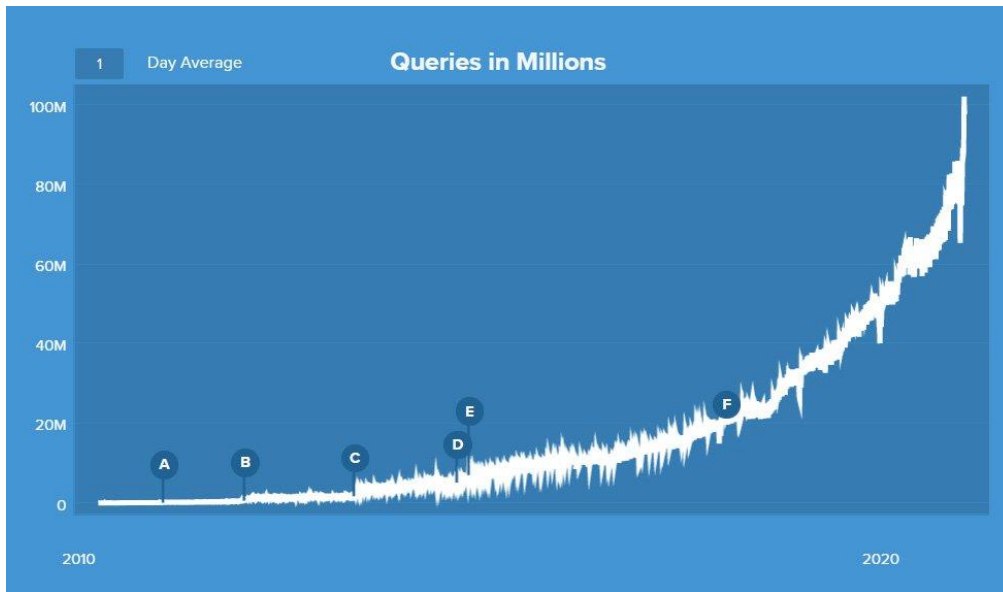
"Each time you search on DuckDuckGo, you have a blank search history, as if you've never been there before," DuckDuckGo explains in their [privacy blog](#).

DuckDuckGo showed 62% growth in 2020

As people are increasingly becoming more concerned about how their data is being used online, DuckDuckGo has seen huge growth on a year-by-year basis.

In a statement to BleepingComputer, DuckDuckGo said that it recorded a 62% growth in average daily searches in 2020. So far, in January 2021, the search engine receives an average of 90 million search queries per day.

On January 11th, 2021, DuckDuckGo received 102,251,307 daily search queries, a record for the search engine.



DuckDuckGo daily search queries
Source: DuckDuckGo

DuckDuckGo attributes its growth to users who are seeking more privacy while using the Internet. With the increasing reports of data breaches, people's data being used for political purposes, or their behavior tracked throughout the Internet, more and more people are switching to the privacy-centric search engine.

"While we don't track our users, we do study user adoption through national surveys. What we've learned from those surveys is that our overall growth is driven by people who want more privacy online via word of mouth conversations," DuckDuckGo told BleepingComputer.

The search engine also told BleepingComputer that high-profile privacy news, such as the recent concerns regarding data sharing between WhatsApp and Facebook, lead to increased traffic for the search engine.

"The recent Facebook / WhatsApp privacy policy announcement seems to have had some impact increasing search similar to how it has driven people to private messaging alternatives like Signal. We've seen this happen before, when a high profile privacy issue is exposed, we generally see an increase in use," DuckDuckGo explained.

According to StatCounter, this increased growth has led DuckDuckGo to become the second most used search engine on mobile devices in the US, UK, CA, and AUS markets.

While Google still commands a 94% market share in the US, DuckDuckGo is now in second place with 2.25%, followed by Yahoo at 1.94%.

Source: <https://www.bleepingcomputer.com/news/technology/privacy-focused-search-engine-duckduckgo-grew-by-62-percent-in-2020/>

5. Malwarebytes says SolarWinds hackers accessed its internal emails

Cybersecurity firm Malwarebytes today confirmed that the threat actor behind the SolarWinds supply-chain attack were able to gain access to some company emails.

"While Malwarebytes does not use SolarWinds, we, like many other companies were recently targeted by the same threat actor," Malwarebytes CEO and co-founder Marcin Kleczynski [said](#).

"We can confirm the existence of another intrusion vector that works by abusing applications with privileged access to Microsoft Office 365 and Azure environments.

"After an extensive investigation, we determined the attacker only gained access to a limited subset of internal company emails."

However, Kleczynski also added that the company did not find evidence of a compromise or unauthorized access to internal production or on-premises environments.

The threat actor behind the SolarWinds hack is tracked as [StellarParticle](#) (CrowdStrike), [UNC2452](#) (FireEye), and [Dark Halo](#) (Volexity), and is [likely a Russian-backed Advanced Persistent Threat \(APT\) group](#) according to a joint statement issued by the FBI, CISA, ODNI, and the NSA earlier this month.

Malwarebytes software is safe to use

Malwarebytes discovered that the threat actor that coordinated the SolarWinds hack used applications with privileged access infiltrate the company's Microsoft Office 365 and Azure environments.

"We received information from the Microsoft Security Response Center on December 15 about suspicious activity from a third-party application in our Microsoft Office 365 tenant consistent with the tactics, techniques and procedures (TTPs) of the same advanced threat actor involved in the SolarWinds attacks," Kleczynski added.

"The investigation indicates the attackers leveraged a dormant email protection product within our Office 365 tenant that allowed access to a limited subset of internal company emails. We do not use Azure cloud services in our production environments."

Malwarebytes software is safe to use given that a thorough analysis of "all Malwarebytes source code, build and delivery processes," did not reveal any signs of unauthorized access or compromise.

Emails accessed via the Microsoft Graph service

The SolarWinds hackers also targeted Malwarebytes administrative and service credentials by adding a self-signed certificate with credentials to the Microsoft Graph service principal account.

This later allowed them to "authenticate using the key and make API calls to request emails via MSGraph."

Malwarebytes is the fourth cybersecurity firm targeted by the [SolarWinds hackers](#), after [Microsoft](#) and [FireEye](#) confirmed that their systems were infiltrated and [CrowdStrike](#) disclosed a failed attack attempt.

"While we have learned a lot of information in a relatively short period of time, there is much more yet to be discovered about this long and active campaign that has impacted so many high-profile targets," Kleczynski said.

"It is imperative that security companies continue to share information that can help the greater industry in times like these, particularly with such new and complex attacks often associated with nation state actors."

Source: <https://www.bleepingcomputer.com/news/security/malwarebytes-says-solarwinds-hackers-accessed-its-internal-emails/>

6. Space Cybersecurity: How Lessons Learned on Earth Apply in Orbit

The universe is getting smaller, and space cybersecurity is keeping up. On May 30, 2020, nearly a decade after the Space Shuttle program ended, people witnessed a first: a vehicle built as part of a public-private partnership (between SpaceX and NASA) took off into space. This development was transformational because it brought the world one step closer to [commercial space travel](#). We now have proof of concept that space travel, once reserved for powerful nation-states, is something that can be achieved, albeit with a lot of assistance right now, by a commercial company.

How safe space travel may be for everyday people is yet to be seen, but it's an exciting time because we can actually start talking space travel, space tourism and [space mining](#).

But space travel is not cheap, and safety is not a joke. The risks that come with space travel mean you do not play games when it comes to redundant and backup options. When making these huge investments, you cannot afford to go bust or risk lives. That means as

people make efforts to go more often and deeper into outer space, cybersecurity becomes a real issue that must be addressed.

Why? Well, think “E.T. phone home” as a start. If you want space travel safety, you have to be able to [communicate](#).

Space and Cybersecurity

On Sept. 4, 2020, the White House issued the [Memorandum on Space Policy Directive-5 — Cybersecurity Principles for Space Systems](#). Section 4, Principles is a worthwhile read for cybersecurity experts. Here is a brief overview of that section:

- Space systems and their supporting infrastructure, including software, should be developed and operated using risk-based, cybersecurity-informed engineering.
- Owners and operators should develop and implement cybersecurity plans for their space systems.
- Protect against unwanted access to critical space vehicle functions.
- Include physical protection measures designed to reduce the risks of a space vehicle’s command, control and telemetry receiver systems.
- Protect against communications jamming and spoofing.
- Protect ground systems, operational systems and data processing systems.
- Adopt appropriate cybersecurity hygiene practices, physical security for automated information systems and intrusion detection methodologies for system elements.
- Manage supply chain risks that affect the cybersecurity of space systems through tracking manufactured products.
- Space system owners and operators should collaborate to promote the development of best practices.
- Security measures should be designed to be effective while permitting space system owners and operators to manage risk tolerances and minimize undue burden. These must be consistent with specific mission requirements, United States national security and national critical functions, space vehicle size, mission duration, maneuverability and any applicable orbital regimes.

For any cybersecurity policy wonk, this is pretty much a dream-come-true list of security principles. But, don’t we try to apply those same principles down here on planet Terra? Yes, we do. Emphasis on the word *try*.

Today's World is Guided by Space Research

Unlike the internet, which is [inherently vulnerable by design](#), there is an opportunity in space to build a uniquely secure means of communication that could not only reduce the dangers of research, but also could alter even land-based communications and way of life. For example, Space Policy Directive-5 gives us plenty of examples of how space research helps with homeland security. We rely on space systems for a lot of things we take for granted in our daily lives:

- Global connections
- Position, navigation and timing
- Scientific research
- Exploration
- Weather tracking
- National defense

The fact that the use of the [NIST Cybersecurity Framework](#) is now 'baked in' to space projects is a welcomed development. But, there is something more intriguing going on with Space Policy Directive-5 and all the Space Policy Directives. Security-by-design principles are a driving force in their creation.

Building Trustworthy Space Cybersecurity Systems

If you haven't heard of security-by-design, think about it like this. In its crudest form, it means to break while you build so you can fix and strengthen the weak spots. If you do this correctly and go above and beyond, you not only strengthen your system, you also build antifragility into your system. Nassim Nicholas Taleb, who [coined the term antifragile](#), says this means the project doesn't merely withstand a shock, but improves because of it.

That's the chance we have with space systems that we don't have with the internet. In fact, the internet is the exact opposite of being antifragile because we keep building on its inherent risks, making it more complex and, in turn, more fragile.

Guidelines and Best Practices

If you're looking for guidance on how to employ security-by-design principles, one of the best resources is [NIST Special Publication 800-160](#), Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.

NIST SP 800-160 is great for future space communication system designs and for those who have the luxury to build their IT systems from scratch. It draws on a wide variety of standards and principles from the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the Institute of Electrical and Electronics Engineers (IEEE).

“Infus[ing] systems security engineering methods, practices and techniques into those systems and software engineering activities,” NIST SP 800-160 allows you to better understand cybersecurity needs and plan for them well.

Security for Telecommunications Networks at the Speed of Light

Let’s take a look at a specific type of project that illustrates the way space cybersecurity professionals can apply to projects on Earth. Here on the ground, [we’re getting all excited about 5G](#), as we should be. But something else exciting is happening when it comes to satellite security: [quantum communications](#). Leaving aside for a moment that we are still early into quantum communications development, or more accurately, quantum key distribution (QKD), QKD in theory — at least in space — should be easier to achieve.

Let’s start with some background, without getting technical. QKD is great when it comes to encryption because a user can identify right away if a message has been tampered with. [In theory](#), QKD is unbreakable, because subatomic particles (photons) act in a very peculiar way. Mess with those particles and the message is no longer secure.

That’s awesome, right? How come we don’t use QKD all the time?

The Problem with Quantum Keys

It’s just not practical. QKD data transfer over long distances and into today’s network is just not feasible on a mass scale. We’re talking distances of a [few kilometers only in some cases](#). But when you add space and satellites into the equation, the metrics change a lot.

Why is that? Well, because of the nature of space and the nature of physics. Ground-based quantum signals suffer from something called rate of absorption. If we are to keep this simple and not go completely down the [entanglement-based quantum cryptography rabbit hole](#), think of it like this: the photons can’t travel that far without becoming compromised in some form or another, which means you have to add repeaters along the way. And that’s not a great idea, at least with current-day systems. You’re going to need a whole bunch of repeaters, which could each be attacked.

So, why is this different when it comes to space cybersecurity?

That rate-of-absorption problem pretty much goes away, because the signals are traveling through empty space. Instead of having capabilities over a few kilometers only, suddenly you can have secure communications linked over a much greater distance, like say [1,000 kilometers](#).

In other words, when traveling through empty space, you don’t really need to worry about going through the different barriers you would find here on Earth. And, because of good ole’ physics, we are living in a completely different domain with a different set of rules. That’s what makes space projects so exciting. Our engineers will not be bound by the

same rules of ground-based communications, meaning that we can employ the lessons learned down here up there, as well.

Why Securing Space Data Matters

Some of the reasons why we should be serious about space cybersecurity are obvious, such as keeping ground-based systems running and addressing national defense concerns. But to be more forward thinking, you need to be a bit more ambitious in your outlook. Space travel provides an entirely new domain to be scouted out. Just like the explorers of ancient and classical times, who traveled to find new worlds across the continents and oceans, we are entering the dawn of a new era.

Along with the thirst for knowledge that drove people out into the vast oceans or through rough terrain, there was something else that was driving them, too. Think for a moment about the Silk Road and other routes that unified Europe and Asia. The driving force behind them was trade and commerce, namely the spice trade between Europe, North Africa and Asia.

We open ourselves to an entirely new universe of possibilities if we can start exploring a territory we haven't before. The possibilities are [transformative](#). But if we are to take advantage of this new domain, we need to have a way to realize a return on investment. That's why both land-based cybersecurity resilience and secure space-based communications matter.

Poor cybersecurity practices will sink the ship, both here on Earth and in space. Poor land-based cybersecurity will result in your standard issues: loss of intellectual property, disruption of operations and [compromised devices](#). Meanwhile, poor space cybersecurity could result in multi-billion dollar losses in one shot because your vehicle is sent off course.

The Excitement of a New Era

We should be excited about this new chapter in space cybersecurity, travel and communications. There are so many lessons we can apply, whether they relate to redundancy, vulnerabilities, encryption or even [artificial intelligence](#). The breakthroughs will not only bring space travel into a new era, but also will change how we send messages here.

We have the chance to build a secure system, correctly, using security-by-design principles. If we are successful, now, at the beginning, we will be able to invest our valuable resources more wisely in the future.

Source: <https://securityintelligence.com/articles/space-cybersecurity-how-lessons-learned-on-earth-apply-in-orbit/>

7. Here's how a researcher broke into Microsoft VS Code's GitHub

This month a researcher has disclosed how he broke into the official GitHub repository of Microsoft Visual Studio Code.

A vulnerability in VS Code's issue management function and a lack of authentication checks enabled the researcher to obtain push access, and write to the repository.

For responsibly reporting the vulnerability, the researcher was awarded a bug bounty award of an undisclosed amount.

Flawed regex, no authentication, code injection in CI scripts

While riding a train, researcher RyotaK discovered a vulnerability in the VS Code's Continuous Integration (CI) script that let him break into Microsoft VS Code's official GitHub repository and commit files.

"I was too bored while I was on the train, so I decided to read the VS Code code. After a while, I noticed that VS Code has a separate repository for CI scripts named `vscode-github-triage-actions`. So I decided to read it," RyotaK told BleepingComputer.

Shortly, the researcher noticed an interesting line in the script that could be exploited in code injection attacks:

```
exec(`git -C ./repo merge-base --is-ancestor ${commit} ${release}`, (err) => {
```

"Of course, there is command injection. But it requires control of the 'commit' variable or the 'release' variable," continued RyotaK in an email interview.

The researcher soon realized the commit variable could be controlled by an attacker due to two reasons:

missing authentication checks within the `closedWith` command (i.e. not checking if the user had the authorization to associate commit hashes with an issue), and

flawed regex expression used to validate the `closedWith` command specified in a closing comment.

The `closedWith` command is used to associate a commit hash with the issue before the commit is closed.

However, a flawed regex expression (shown below) used to validate the closing comments and no authentication checks in the CI script meant, any user could associate a commit with an issue, and inject code within the closedWith value.

```
const closingHashComment = /(?:\\|V)closedWith (\S*)/
```

Because VS Code's vulnerable CI workflow ran once a day, around midnight, the researcher carefully planned a Proof-of-Concept (PoC) exploit in advance, so as to not make any dangerous mistakes during night hours.

To do so, the researcher browsed through the GitHub Actions code files for the project to get an understanding of the Continuous Integration and Continuous Delivery (CI/CD) workflow.

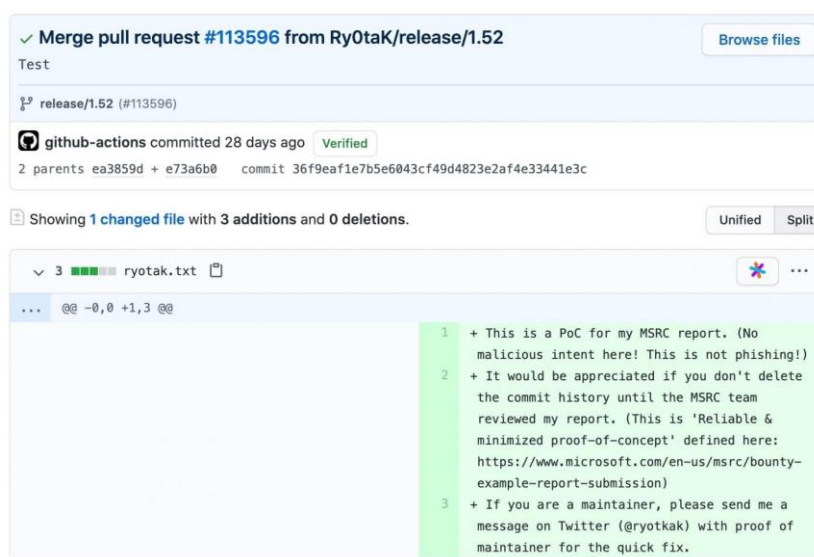
"Fortunately, the workflow files for GitHub Actions are published on GitHub, so I have some idea of what's going on inside GitHub Actions."

"Since actions/checkout was executed in the step before the vulnerable workflow file is used, there was a GitHub token with write permission to the repository. So I made a plan to use this token," the researcher told BleepingComputer.

By injecting his basic PoC exploit into the VS Code's CI script which ran around midnight, the researcher obtained a reverse shell.

Further, the researcher obtained the GitHub authorization token for VS Code repository that would give him write access to the repository.

Eventually, after obtaining the token, the researcher posted a PoC commit to the repository:



Ryotak successfully committed to Microsoft VS Code's GitHub repo by exploiting the flaws

Although, the master branch of the repository had account-based branch protections that could not be bypassed with the GitHub Actions token, it was possible to push the file to the [release](#) branch using the token, states the researcher.

It is worth noting *RyotaK* performed this PoC exploit while adhering to Microsoft's "[safe harbor](#)" guidelines when reporting vulnerabilities through their bug bounty programs.

"Microsoft permits the diagnosis of vulnerabilities through safe harbors. This article describes the vulnerabilities discovered / reported in compliance with the safe harbor, and is not intended to recommend unauthorized vulnerability diagnosis," stated *RyotaK* in his [blog post](#).

For his discovery of the vulnerability and following responsible disclosure guidelines, the researcher told BleepingComputer, that he was awarded a cash bounty prize of an undisclosed amount by Microsoft.

Code repo flaws may pave ways for software supply chain attacks

Flaws of this extent that enable adversaries to break into otherwise secure software codebases can lay the groundwork for sophisticated software supply chain attacks.

This astounding discovery comes to light when the SolarWinds supply chain attack incident has already been making headlines.

In this case, the ethical hacker *RyotaK* discovered and responsibly reported the flaw to Microsoft before advanced threat actors could exploit it, to push their malicious code upstream into the Visual Studio Code repository.

Corruption of [source-code editors and IDEs](#) in a targeted supply chain attack can have devastating consequences for its users, developers, and the clients that would then be receiving the applications built using a tainted IDE.

Recently, another group of security researchers reported finding exposed Git credentials due to improperly secured .git directories on UN domains.

This discovery enabled them to clone the entire Git repository of the [United Nations Environment Programme \(UNEP\)](#) and eventually access over 100,000 employee records.

Securing your CI/CD tools, and proactively auditing their scripts for security flaws before adversaries exploit any vulnerabilities are a few defenses towards preventing software supply-chain compromises.

Source: <https://www.bleepingcomputer.com/news/security/heres-how-a-researcher-broke-into-microsoft-vs-codes-github/>

8. Here's how law enforcement's Emotet malware module works

New research released today provides greater insight into the Emotet module created by law enforcement that will uninstall the malware from infected devices in April.

On January 27th, Europol announced that a joint operation between law enforcement agencies from Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada, and Ukraine [took control of the Emotet botnet's servers](#) and disrupted the malware's operation.

After the takedown, [researchers noticed](#) that the Emotet botnet began to push down a module to infected devices that would uninstall the malware on April 25th, 2021, at 12:00 and later.

On the 28th, it was confirmed in a US Department of Justice press release that "foreign law enforcement" created this module.

"Foreign law enforcement, working in collaboration with the FBI, replaced Emotet malware on servers located in their jurisdiction with a file created by law enforcement, according to the affidavit. This was done with the intent that computers in the United States and elsewhere that were infected by the Emotet malware would download the law enforcement file during an already-programmed Emotet update," states a Department of Justice [press release](#).

In a conversation with Europol and later emails with Germany's Bundeskriminalamt (BKA) federal police agency, we learned that the BKA was responsible for the module.

"Within the framework of the criminal procedural measures carried out at international level, the Bundeskriminalamt has arranged for the malware Emotet to be quarantined in the computer systems affected. An identification of the systems affected is necessary in order to seize evidence and to enable the users concerned to carry out a complete system clean-up to prevent further offences. For this purpose, the communication parameters of the software have been adjusted in a way that the victim systems no longer communicate with the infrastructure of the offenders but with an infrastructure created for the seizure of evidence." - German Bundeskriminalamt

What Malwarebytes' analysis reveals

While we now knew that the module pushed down to infected devices was created by law enforcement to uninstall the malware, there were still some questions unanswered.

For example, why was the uninstall occurring two months away, and what happens before the April 25th, 2021 uninstall date?

Today, [a new analysis](#) by [Jérôme Segura](#) and [hasherezade](#) of Malwarebytes answers some of these questions.

The new Emotet module distributed by German law enforcement is a 32-bit DLL named 'EmotetLoader.dll.'

Offset	Name	Value	Meaning
49DF0	Characte...	0	
49DF4	TimeDate...	FFFFFFFF	niedziela, 07.02.2106 06:28:15 UTC
49DF8	MajorVer...	0	
49DFA	MinorVer...	0	
49DFC	Name	4AC36	EmotetLoader.dll
49E00	Base	1	
49E04	NumberO...	3	
49E08	NumberO...	3	
49E0C	AddressO...	4AC18	
49E10	AddressO...	4AC24	
49E14	AddressO...	4AC30	

Exported Functions [3 entries]				
Offset	Ordinal	Function RV	Name RVA	Name
49E18	1	5940	4AC47	Control_RunDLL
49E1C	2	5940	4AC56	RunDLL
49E20	3	5940	4AC5D	ShowDialogA

*New Emotet module
Source: Malwarebytes*

Below you can see the routine that checks for the date, and if it's April 25th or later, removes Emotet. For more information about the deadline variable, you can reference this [Microsoft documentation](#).

```

1 HANDLE uninstall_in_april()
2 {
3     __time64_t deadline_val; // rax
4     HANDLE result; // eax
5     __time64_t time; // [esp+0h] [ebp-10h] BYREF
6
7     deadline.tm_year = 121;
8     deadline.tm_mon = 3;
9     deadline.tm_mday = 25;
10    deadline.tm_hour = 12;
11    deadline.tm_min = 0;
12    __time64(&time);
13    deadline_val = _mktime64(&deadline);
14    *(double *)&time = _difftime64(time, deadline_val);
15    if ( *(double *)&time > 0.0 ) // did the deadline pass?
16        !uninstall_emotet();
17    result = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)uninstall_emotet_thread, 0, 0, 0);
18    if ( result != (HANDLE)-1 )
19        result = (HANDLE)CloseHandle(result);
20    return result;
21 }

```

Function to uninstall on April 25th, at 12:00

When removing Emotet, Malwarebytes states the uninstaller deletes only the associated Windows services, deletes its autorun Registry key, and then exits the process.

On the other hand, prior to April 25th, 2021, the module allows Emotet to be installed on the device.

However, the difference is that the Emotet command and control server is now configured to use law enforcement servers located in Germany. As law enforcement controls the botnet, Emotet will not download further modules to the infected PC to perform malicious activity.

"Well, it still loads Emotet but with a big difference. It swaps the C2s for those controlled by LE. So your machine, while it waits for the cleanup to activate, will ping LE servers." Segura told BleepingComputer.

Malwarebytes states that this new module will be pushed down to all infected devices, effectively replacing the malicious Emotet installs already infecting their computers.

"For victims with an existing Emotet infection, the new version will come as an update, replacing the former one. This is how it will be aware of its installation paths and able to clean itself once the deadline has passed," explains Malwarebytes.

What is still not answered is why wait two months to uninstall the malware rather than doing it immediately?

Based on the BKA's statement, it is likely being done to allow law enforcement to gather further evidence, such as the number of infected devices infected and what countries these devices are located. It could also be used to identify corporate victims to warn them of further potential compromises of their networks.

BleepingComputer's attempts to get official answer to this question has been unsuccessful.

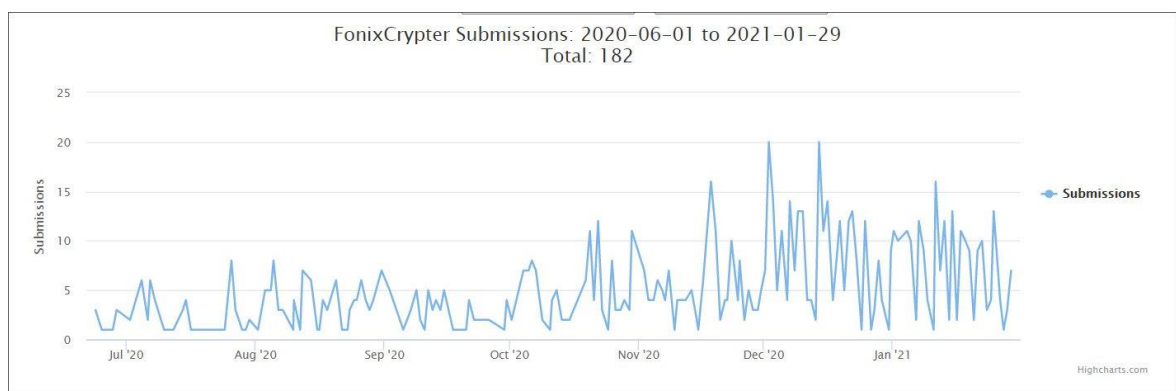
"Please understand that we cannot provide any further information as the investigations are still ongoing," the German BKA told BleepingComputer in response for more information.

Source: <https://www.bleepingcomputer.com/news/security/heree-how-law-enforcements-emotet-malware-module-works/>

9. Fonix ransomware shuts down and releases master decryption key

The Fonix Ransomware operators have shut down their operation and released the master decryption allowing victims to recover their files for free.

Fonix Ransomware, also known as Xinof and FonixCrypter, began operating in June 2020 and has been steadily encrypting victims since. The ransomware operation was not as widely active as others, such as REvil, Netwalker, or STOP, but starting in November 2020, it picked up a bit, as shown by the ID Ransomware submissions below.



ID Ransomware submission stats

This afternoon, a Twitter user claiming to be a Fonix ransomware admin announced that the ransomware had shut down.



Tweet from Fonix admin

The message shared in the image reads:

*I'm one fonix team admins.
you know about fonix team but we have come to the conclusion.
we should use our abilities in positive ways and help others.
Also rans0mware source is completely deleted, but some of team members are disagree with closure of the project, like telegram channel admin who trying to scam people in telegram channel by selling fake source and data.
Anyway now main admin has decided to put all previous work aside and decrypt all infected systems at no cost.
And the decryption key will be available to the public.
The final statement of the team will be announced soon.*

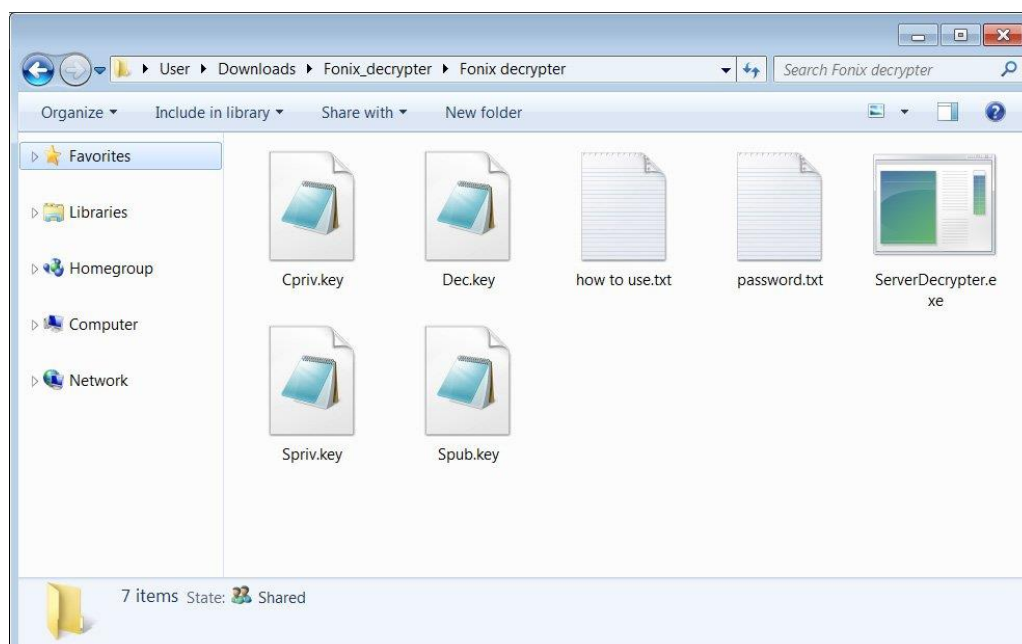
Regards-FonixTeam

According to the message, some of the 'members' of the ransomware operation were not happy that it was shutting down.

This shutdown could cause members to join other ransomware affiliate programs or splinter off and create a new operation.

Master keys work, decryptor is a mess

In a [different tweet](#), the Fonix admin shared a link to a RAR archive named 'Fonix_decrypter.rar' containing both a decryptor and the master private decryption key.

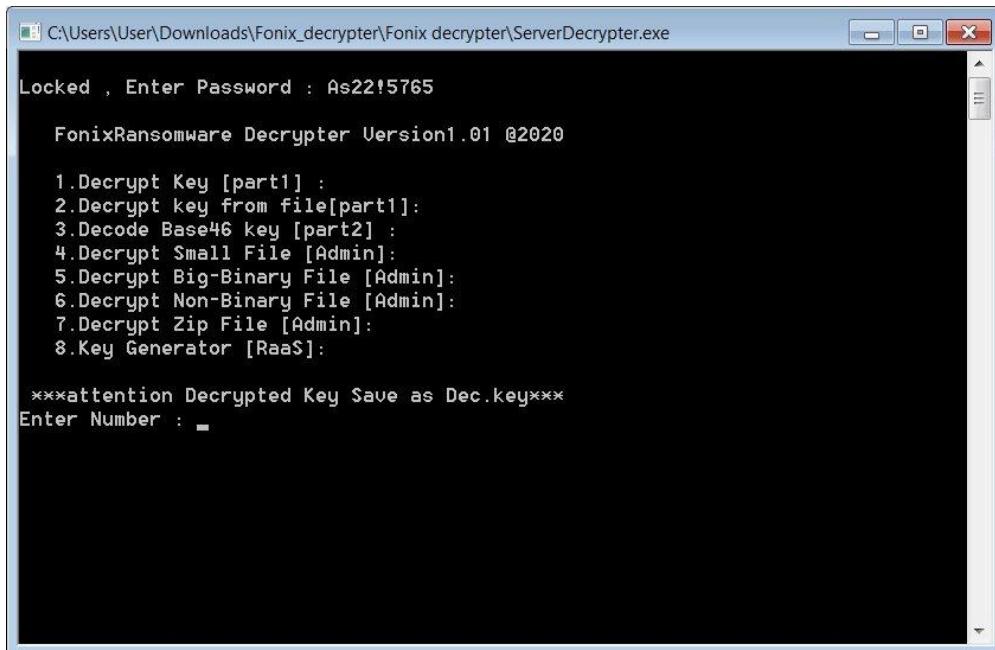


Fonix Decryptor archive

This decryption tool is not a decryptor that can be used by a victim to decrypt their files easily but is instead an admin tool used internally by the ransomware gang.

Most ransomware operations allow victims to send a few encrypted files that they will decrypt for free to prove that they can do so.

The decryptor released tonight is the Fonix Ransomware operators' tool when performing these free test decryption and does not allow a victim to decrypt an entire computer.



```
C:\Users\User\Downloads\Fonix_decrypter\Fonix_decrypter\ServerDecrypter.exe
Locked , Enter Password : As22!5765

FonixRansomware Decrypter Version1.01 @2020

1.Decrypt Key [part1] :
2.Decrypt key from file[part1]:
3.Decode Base46 key [part2] :
4.Decrypt Small File [Admin]:
5.Decrypt Big-Binary File [Admin]:
6.Decrypt Non-Binary File [Admin]:
7.Decrypt Zip File [Admin]:
8.Key Generator [RaaS]:

***attention Decrypted Key Save as Dec.key***
Enter Number : _
```

Fonix ransomware's Admin decryptor

Even considering that it can only decrypt one file simultaneously, from our tests of the decryptor, it has very confusing instructions and is prone to crashing.

The good news is that Michael Gillespie has told BleepingComputer that the master keys work but only on some Fonix ransomware versions.

However, Emisoft's decryptor will decrypt all versions of the ransomware, which include the .Fonix, .FONIX, .repter, .XINOF encrypted file extensions.

There is no ETA as to when the decryptor will be released, but if you are a victim of this ransomware, a solution will be available soon.

Source: <https://www.bleepingcomputer.com/news/security/fonix-ransomware-shuts-down-and-releases-master-decryption-key/>

10. Data of 66,000 users left open on a misconfigured Elasticsearch server

VIPGames, a free platform with a total of 56 available classic board and card games like Hearts, Crazy Eights, Euchre, Dominoes, Backgammon and others, has exposed the personal data of tens of thousands of users. While the game publisher acknowledges the potential for user data exfiltration, it maintains that there is no evidence data was actually leaked.

In all, more than 23 million records for more than 66,000 users were left exposed thanks to a cloud misconfiguration, according to a report from WizCase. Aside from its desktop users, VIPGames has mobile players too, including via an app that's been downloaded from the Google Play store more than 100,000 times alone.

The site joins a growing list of companies caught without properly configured clouds which can lead to disastrous results for customers.

In a statement, released after this original Threatpost report was published, [VIPGames acknowledged](#) "an issue that potentially exposed user profiles" but stated it wasn't aware any user data was leaked.

"We would like to clarify that this was a temporary misconfiguration, NOT an attack, hack, or breach. There are no records of any data being leaked. This misconfiguration was disclosed to us by a team of white hat penetration testers," the company publicly stated. "The misconfiguration was resolved in less than two hours. Information about this was responsibly disclosed by the team at WizCase – cyber security research team."

The WizCase research team, led by Ata Hackl, regularly scans the internet for open servers and found the sensitive [personal information exposed](#) and available to any cybercriminal who happened to stumble across it.

Online gaming represents a particularly desirable set of personal details for cybercriminals, the report explained.

Leaky Gamer Clouds Particularly Dangerous

"Online gaming brings together user personal information, transaction details and gaming habits. This fusion of confidential information creates a lucrative environment for cybercriminals to exploit," the WizCase report explained. "Gaming platforms routinely experience multiple attacks from hackers, sabotage from competing platforms, intra-platform attacks by players targeting the Internet connections of rival users, and more."

In this case, the site's unprotected server leaked more than 30GB of data containing 23 million individual records, including usernames, emails, IP addresses, hashed passwords, Facebook, Twitter and Google IDs, bets and even data on players who were banned from the platform, WizCase said.

"Each of these data sets is not just valuable on its own but can also be used to map out other information," the report explained. "For example, from the player IDs, it's possible for an attacker to locate the player's email address, IP address and hashed password, which is particularly relevant for the banned players."

The report added that the VIPGames Terms of Use explains players can be blocked from the platform for bad behavior or cheating, and that the exposed records included the dirty details of each infraction.

"Some of these included potential pedophilia and exhibitionism," WizCase said, adding potential blackmail to the list of threats the exposed data posed to users, in addition to identity theft, password breaches, phishing scams, malware and more.

"Their report brought to attention an Elasticsearch server misconfiguration that occurred with one of our servers that was part of our backup log and stored user data older than six months. The event took place on October 5th, and it was resolved within two hours by our team," VIPGames said in its statement. "We have since revised our stack to no longer include this type of data storage in any of our environments. Additionally, our team has implemented further improvements to secure all user data."

This breach represents a wider trend of [companies failing to lock-down their data](#) in the cloud.

Misconfigured Clouds Are Everywhere

Last September high-end gaming gear company Razer left the personal data of about [100,000 users exposed](#) on a similar Elasticsearch cloud cluster.

That same month, a group of 70 different adult dating sites was also discovered to be storing sensitive personal data — like sexual preferences — on an [unsecured Elasticsearch server](#), leaking more than 320 million individual records.

In April, the Key Ring digital wallet app exposed 44 million customer records including IDs, charge cards, loyalty cards, gift cards and membership cards left [open on an Amazon Web Services S3 server](#). And last summer, [Joomla exposed the data](#) of 2,700 people signed up for the Joomla Resources Directory community forum in an unsecured Amazon Web Services cloud storage bucket.

Palo Alto Networks' Unit 42 estimates about 60 percent of breaches occur because of misconfigured public clouds.

Ryan Olson, vice president of threat intelligence with the Unit 42 team, explained that while 86 percent of companies deploy cloud apps, only 34 percent have "single sign-on (SSO) solutions in place, demonstrating a massive gap in cloud adoption and necessary cloud-security solutions."

As for users, experts agree basic best practices for online security are always a good idea — be careful about what you share, avoid clicking on suspicious emails or links and proper password hygiene are important, WizCase advised. The firm also suggested using a VPN service to keep location data secure and install good antivirus software while the industry struggles to keep up.

“The use of the cloud enables organizations to reach their goals and scale with ease,” Anurag Kahol, CTO at Bitglass, said via email. “As more organizations adopt cloud-based tools to obtain a competitive advantage, the rate of cloud-application usage increases in tandem. However, most organizations are not equipped to handle the security demands of the cloud.”

Source: <https://threatpost.com/gamer-records-exposed-vipgames-leak/163352/>

11. Microsoft Edge, Google Chrome Roll Out Password Protection Tools

Two major browsers –Microsoft Edge and Google Chrome – are rolling out default features, which they say will better help notify users if their password has been compromised as part of a breach or database exposure.

Edge and Chrome’s moves signify a bigger push by browsers to solve the [big “password problem”](#) plaguing the security industry. Over the past two years, major browsers (including [Mozilla Firefox](#)) have launched built-in tools for helping users identify passwords that are increasingly wrapped up in data breaches – and easily change them.

Microsoft Password Monitor

Microsoft [on Thursday](#) said that its next version of Edge (version 88.0.705.50) will generate alerts if a user password is found in an online leak. The tool, called Password Monitor, will check users’ passwords against a data repository of known, breached credentials. If the passwords saved to the browser matches those on a list of leaked credentials, Password Monitor will send users alerts and prompt them to update their password.

“To ensure security and privacy, user passwords are hashed and encrypted when they’re checked against the database of leaked credentials,” said Microsoft.

In addition, Microsoft’s newest Edge version will include a built-in “strong password generator,” which it hopes will promote strong passwords for internet users who are signing up for a new account, or changing an existing password.

Security experts applauded the new measures. “By having the password management feature in the browsers look for compromised credentials, it allows the potential victim to change the password in other places before it impacts them,” Erich Kron, security awareness advocate at KnowBe4 told Threatpost. “Hopefully, it will also demonstrate to the individual the importance of not reusing passwords across multiple services.”

Google Chrome’s Latest Password Protections

Meanwhile, [Google this week announced](#) it will introducing new features that will consolidate its password protections – and make them for seamless for users – in Chrome 88 over the coming weeks. Chrome 88 will give allow users to launch a simple check to identify any weak passwords and “take action easily.” By navigating to the top of their browser and clicking on passwords and “Check Passwords,” users are able to easily check whether all of their passwords have been compromised in a breach – and on the same page edit their passwords to choose safer alternatives if need be.

Chrome [already alerts users if their passwords have been compromised](#) and prompts them to update – However, the idea here is to give users the ability to update multiple usernames and passwords easily all in one place.

“That’s why starting in Chrome 88, you can manage all of your passwords even faster and easier in Chrome Settings on desktop and iOS (Chrome’s Android app will be getting this feature soon, too),” said Google.

Chrome also provided an update on its existing password protection tools, including Safety Check, launched in 2020, which tells Chrome users if passwords they’ve asked the browser to remember have been compromised. Google said as a result of Safety Check it has seen a 37 percent reduction in compromised credentials stored in Chrome.

Password Health Continues to Fail

With data breaches continuing to hit companies, attackers are accessing credentials across the board. However, compromised data isn’t leading to actionable changes by consumers – in fact [a 2020 survey found that half of respondents](#) hadn’t changed their password in the last year – even after they heard [about a data breach](#) in the news. This “password problem” has challenged the security industry for years, with companies grappling with issues like poor password hygiene, password reuse or easy-to-guess passwords. Making matters worse, passwords are appearing left and right online as part of major data breaches – yet victims aren’t changing their passwords at all across various platforms. The [Collection #1](#) data dump in 2019 for instance, which included 773 million credentials, and subsequent [Collection #2-5 dumps](#), show exactly how many passwords are available on the Dark Web and underground forums.

“Password compromise is a huge ongoing issue leading to everything from data breaches to ransomware or other malware infections,” Kron said. “This in large part due to the

practice of credential stuffing. This is where cybercriminals take known usernames and passwords from previous breaches and attempt to use them on other services. Knowing that people tend to reuse passwords across multiple services, they know the odds of success are worth the effort.”

Lamar Bailey, senior director of security research with Tripwire, said that passwords are “the Achilles heel of cybersecurity.”

“The vast majority of breaches start with stolen, weak or reused passwords,” Bailey said. “Our brains can’t keep up with a long list of passwords that map to all of the various sites, assets and services we access on a given day. Third-party password vaults... have become the de facto standard to solve this problem. With the latest update, Chrome and Edge will be competing with these third-party products by offering some of the same features.”

Source: <https://threatpost.com/microsoft-edge-google-chrome-roll-out-password-protection-tools/163272/>

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.