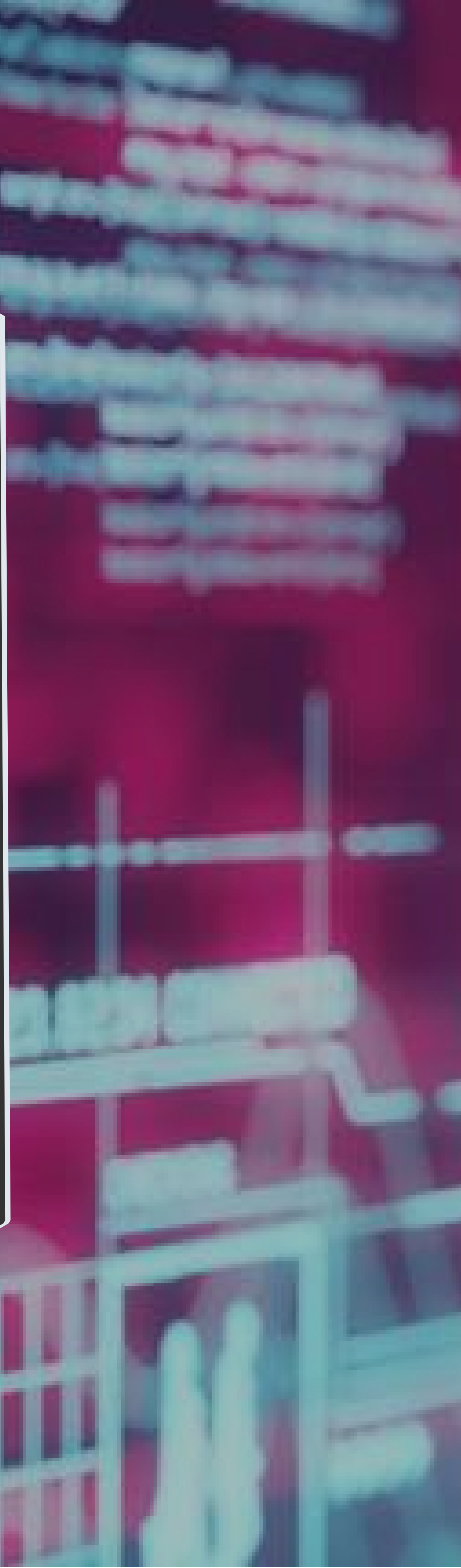


PURPLESEC

CYBER SECURITY INGEST

MAY 31, 2022

Analysis from

PurpleSec's Security Experts

AI POWERED PENETRATION TESTING

PURPLESEC

HOW IT WORKS WITH PURPLESEC

Our pen testers come equipped with enhanced Artificial Intelligence

We send an onsite device, or send you an agent with a simple 1 day setup

We scan, fingerprint, then launch social engineering campaigns and attacks

Our tools use MITRE's ATT&CK framework to simulate typical attacks

Our security experts provide immediate and actionable results

ACTIONABLE RESULTS IN 2 WEEKS

STARTING AT $10,000

Get enterprise grade penetration testing at an affordable price

LEARN MORE

purplesec.us | 2151 Tannin PL, Vienna, VA 22182 | sales@purplesec.us |

ABOUT PURPLESEC

PurpleSec is a veteran owned and led cyber security company based in Vienna, Virginia just outside of Washington, DC.

Our cyber security experts have received extensive experience and training from operations serving in:

- **U.S. Cyber Command**
- **Department of Defense**
- **Special Operations**
- **Private Industries**
- **Healthcare IT**

Now we're bringing the best of breed practices to the commercial marketplace.

Our proven methods backed by experts work to seamlesslessly integrate security into your existing business processes.

Ultimately, our goal is to provide enterprise level security for SMBs that go beyond the typical compliance checkboxes.

SPEAK WITH AN EXPERT

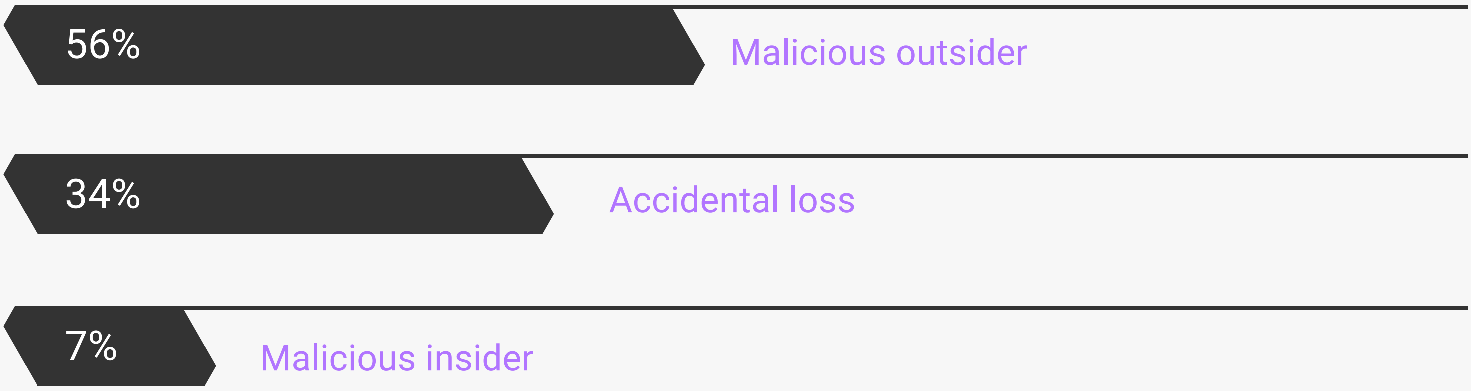
CONTENTS

CYBER SECURITY STATISTICS

We share a handful of cyber security statistics across the industry that we think you might be interested in. From the cost of cybercrime to the rise of supply chain attacks, our library of expertly curated security statistics has you covered:

Cybercrime growth since the beginning of the pandemic: **600%**

THE TOP NUMBER OF BREACH INCIDENTS (SOCIAL ENGINEERING)



Number of cyber attacks per day	Cost of ransomware damage in 2019	Malicious mobile apps blocked every day
80,000	$11.5B	24,000

RECENT CYBER ATTACKS & DATA BREACHES

As data breaches become more pervasive in our interconnected world so must our understanding of modern day cyber attacks.

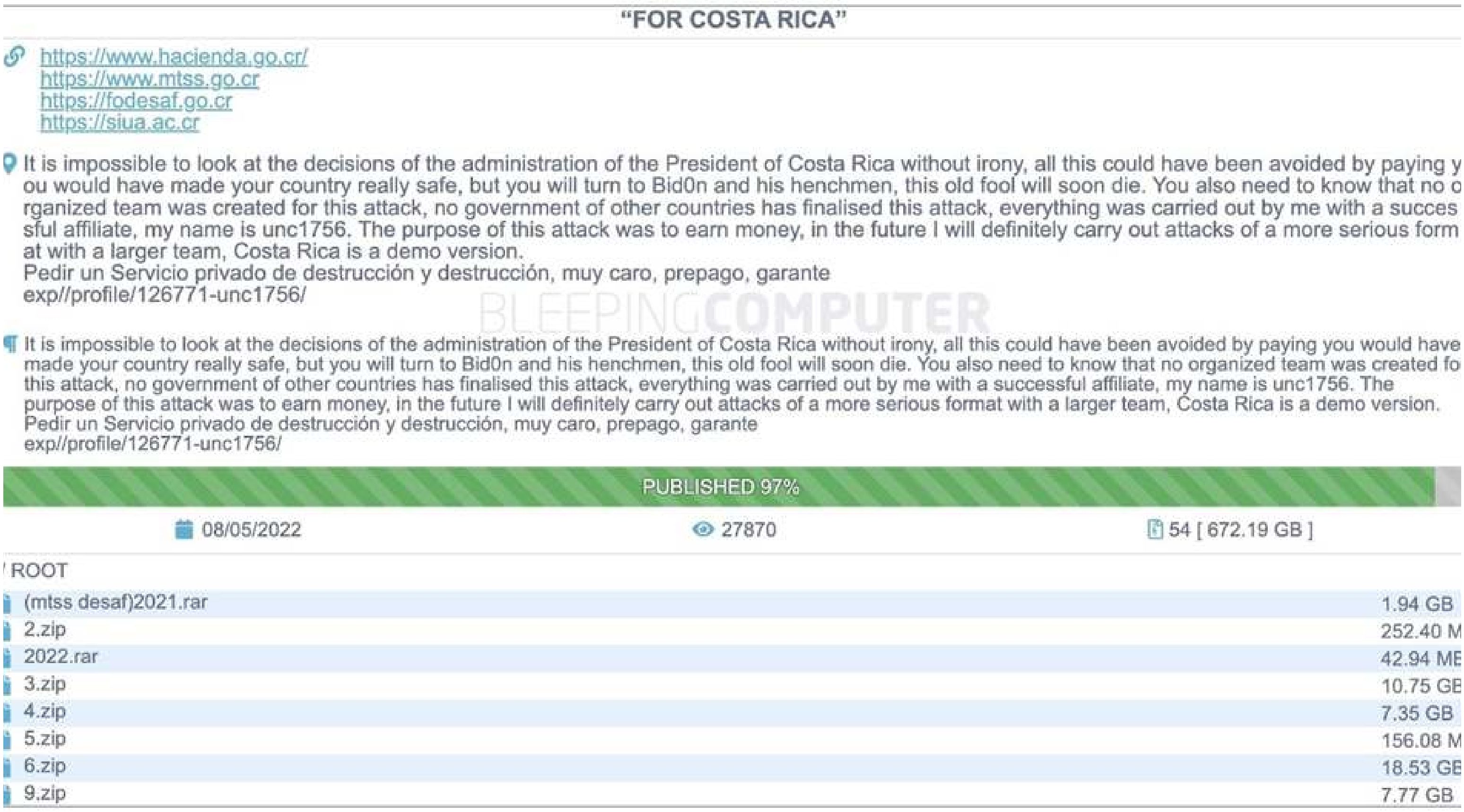
In this series, we sit down with cyber security experts and get their take on the most recent and relevant cyber attacks and breaches.

In this month's issue we cover:

- Conti Costa Rica Emergency

CONTI COSTA RICA EMERGENCY

Analysis by: Josh Allen



"FOR COSTA RICA"

https://www.hacienda.go.cr/
https://www.mtss.go.cr
https://fodesaf.go.cr
https://siua.ac.cr

It is impossible to look at the decisions of the administration of the President of Costa Rica without irony, all this could have been avoided by paying you would have made your country really safe, but you will turn to Bid0n and his henchmen, this old fool will soon die. You also need to know that no organized team was created for this attack, no government of other countries has finalised this attack, everything was carried out by me with a successful affiliate, my name is unc1756. The purpose of this attack was to earn money, in the future I will definitely carry out attacks of a more serious format with a larger team, Costa Rica is a demo version.
Pedir un Servicio privado de destrucción y destrucción, muy caro, prepago, garante
exp//profile/126771-unc1756/

It is impossible to look at the decisions of the administration of the President of Costa Rica without irony, all this could have been avoided by paying you would have made your country really safe, but you will turn to Bid0n and his henchmen, this old fool will soon die. You also need to know that no organized team was created fo this attack, no government of other countries has finalised this attack, everything was carried out by me with a successful affiliate, my name is unc1756. The purpose of this attack was to earn money, in the future I will definitely carry out attacks of a more serious format with a larger team, Costa Rica is a demo version.
Pedir un Servicio privado de destrucción y destrucción, muy caro, prepago, garante
exp//profile/126771-unc1756/

PUBLISHED 97%

08/05/2022 | 27870 | 54 [672.19 GB]

/ ROOT

(mtss desaf)2021.rar	1.94 GB
2.zip	252.40 M
2022.rar	42.94 M
3.zip	10.75 G
4.zip	7.35 GB
5.zip	156.08 M
6.zip	18.53 G
9.zip	7.77 GB

Image credit: *BleepingComputer*

- Costa Rica was attacked by Conti in April 2022.
- After the initial ransom demands were rejected, several ministries and agencies have since been attacked.
- Over 600GB of data stolen from the attack has been leaked online
- Costa Rica has declared a state of emergency as a result of the impact of the incident.
- The US Department of State is offering a $15 million bounty for the arrest of those responsible for deploying Conti.

CONTI COSTA RICA EMERGENCY

Analysis by: Josh Allen

On May 8th, 2022 the President of Costa Rica Rodrigo Chaves declared a national emergency due to an ongoing Conti ransomware campaign against several Costa Rican government entities starting in April of this year.

Conti is a prolific ransomware-as-a-service operation that has been infecting and damaging systems since it was first observed in 2020. Attributed to the threat group called WizardSpider by CrowdStrike in 2019.

The group is also known for TrickBot and the Ryuk ransomware distributed through the ZLoader botnet which we previously reported as shutdown by Microsoft. Conti ransomware contains new and novel techniques that few other ransomware variants have exhibited so far.

Conti's design makes it one of the fastest encrypting ransomware, able to run 32 simultaneous encryption threads, and it can be remotely controlled via command-line options.

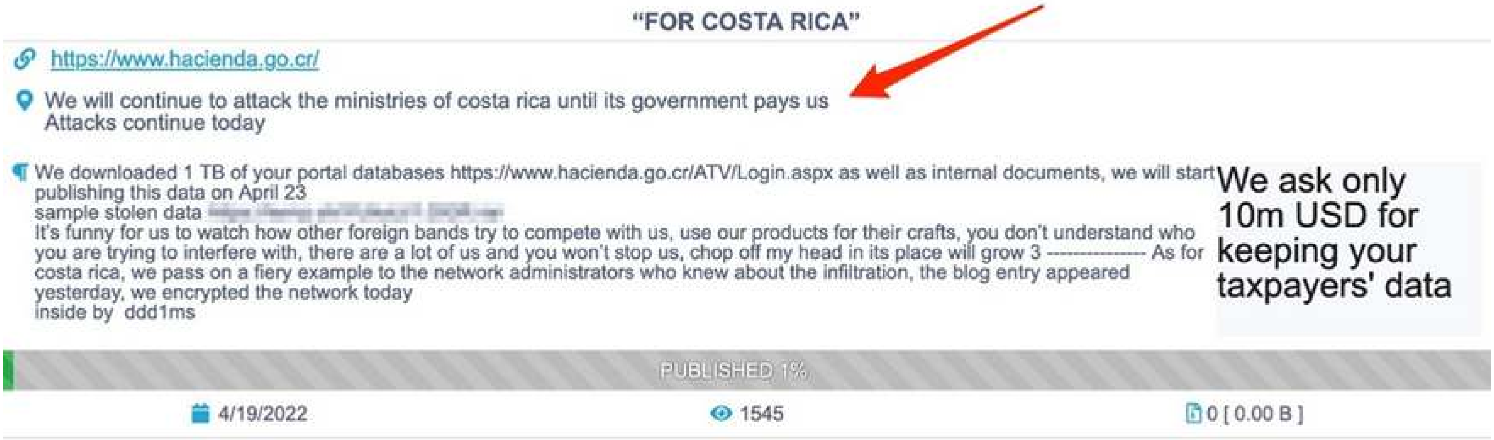
Attackers are able to target and control what files are encrypted and in what order, allowing the malware to quickly encrypt important shared data without immediately making the local system unusable to users which could allow an enterprise time to act.

CONTI COSTA RICA EMERGENCY

Analysis by: Josh Allen

The attack on the nation of Costa Rica began with a Conti cyber attack at the Ministry of Finance on April 18th. The Ministry is still evaluating the scope of the incident and has yet to determine what, if any, impact there may be on taxpayers' information or payments. **Conti demanded $10 million USD or they would continue to attack the nation's Ministries**.

Costa Rica's government **declined to pay the initial ransom**. Keeping good on their promise, WizardSpider continued its campaign and has so far infected the Administrative Board of the Electrical Service of the province of Cartago (Jasec); the Ministry of Science, Innovation, Technology and Telecommunications; the Ministry of Labor and Social Security (MTSS); as well as the National Meteorological Institute (IMN), Radiographic Costarricense (Racsa), The Interuniversity Headquarters of Alajuela, The Social Development and Family Allowances Fund (FODESAF) and the Costa Rican Social Security Fund (CCSS). All of these agencies have had their operations impacted in some way.



"FOR COSTA RICA"

https://www.hacienda.go.cr/

We will continue to attack the ministries of costa rica until its government pays us
Attacks continue today

We downloaded 1 TB of your portal databases https://www.hacienda.go.cr/ATV/Login.aspx as well as internal documents, we will start publishing this data on April 23
sample stolen data [redacted]
It's funny for us to watch how other foreign bands try to compete with us, use our products for their crafts, you don't understand who you are trying to interfere with, there are a lot of us and you won't stop us, chop off my head in its place will grow 3 -------------- As for costa rica, we pass on a fiery example to the network administrators who knew about the infiltration, the blog entry appeared yesterday, we encrypted the network today
inside by ddd1ms

We ask only 10m USD for keeping your taxpayers' data

PUBLISHED 1%

4/19/2022 1545 0 [0.00 B]

Image credit: BetterCyber

CONTI COSTA RICA EMERGENCY

Analysis by: Josh Allen

BleepingComputer reports that as of May 9th, **Conti has leaked over 97% of a 672GB data dump which allegedly contains information stolen from the government agencies**. Conti has the capability to make and exfiltrate copies of any data that in encrypt, which can turn a ransom campaign into an extortion attempt even after the encrypted files are restored.

Conti is just one example of ransomware. There are many other well-known variants and new ones are being created all the time. It is important to take ransomware seriously at your business.

To protect yourself from ransomware PurpleSec recommends:

The Cybersecurity and Infrastructure Security Agency (CISA) raised the alarm about Russian state-sponsored cyber-attacks once again in late April.

- **Read** How to Prevent Ransomware Attacks: An Expert Guide
- **Implement** PurpleSec's Cyber Security Maturity Model for Business
- **Complete** an Internal Penetration Test to understand your attack surface
- **Contact Us** for Vulnerability Management Services

Conti is just one example of ransomware. There are many other well-known variants and new ones are being created all the time. It is important to take ransomware seriously at your business.

The full extent of the continuing attack, the leak, and its impact on the citizens of Costa Rica has yet to be determined. The declaration of national emergency has given the government of Costa Rica some national powers to help defend itself from the attack and recover from any damages.

In a separate but related announcement last week, **the U.S Department of State is offering $10 million for information that identifies** and locates anyone related to Conti, with an **additional $5 million bounty** for information leading to the arrest of those directly responsible for creating and delivering Conti attacks.

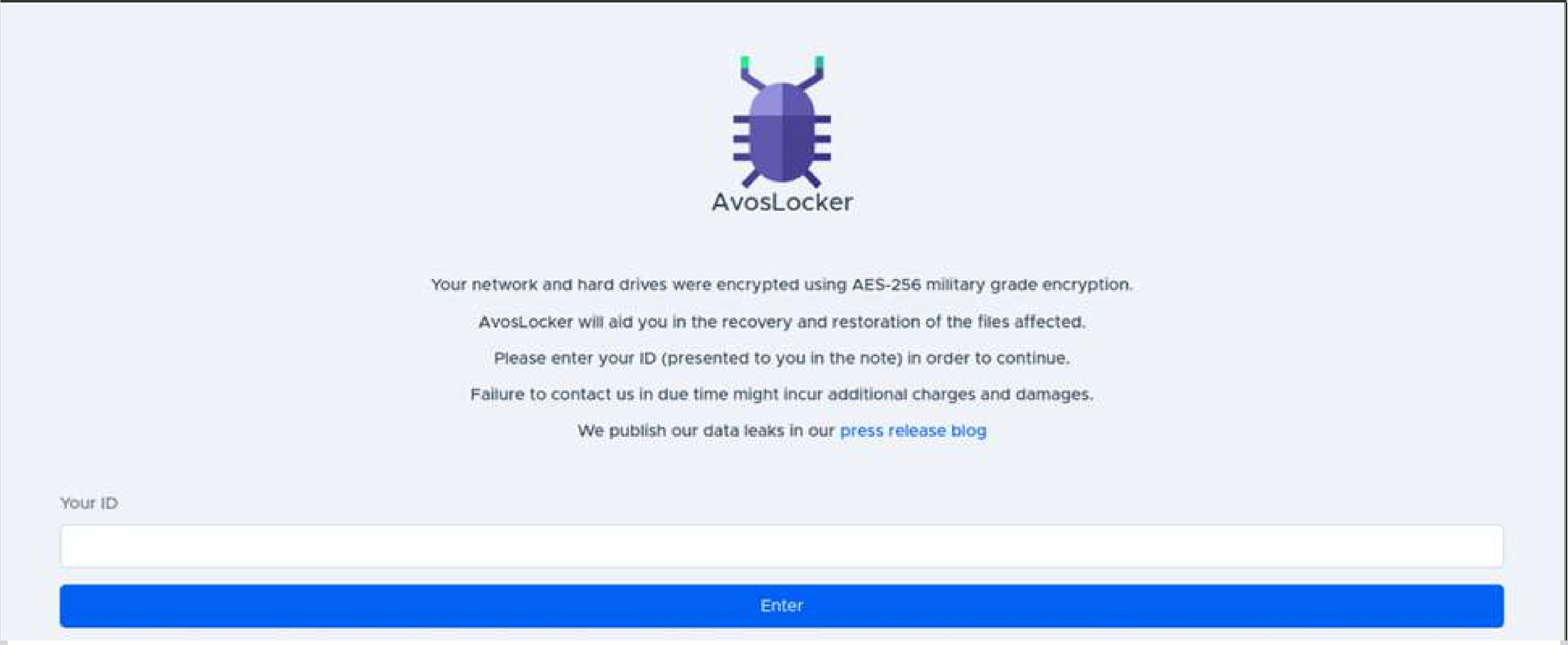
SECURITY RESEARCH

Security researchers around the globe are constantly publishing new findings on techniques, malware, and other trends that are critical to understanding for modern day cyber defense.

With hundreds of publications being published on a weekly basis, it can be difficult to know what research needs to be kept top of mind. In this series, our experts sift through the noise and analyze only the top research you need to know.

In this month's issue we cover:

- AvosLocker Ransomware
- Nimbuspwn Vulnerability



AvosLocker

Your network and hard drives were encrypted using AES-256 military grade encryption.
AvosLocker will aid you in the recovery and restoration of the files affected.
Please enter your ID (presented to you in the note) in order to continue.
Failure to contact us in due time might incur additional charges and damages.
We publish our data leaks in our press release blog

AvosLocker is a Ransomware as a Service (RaaS) affiliate-based group that has targeted victims across multiple critical infrastructure sectors in the United States including, but not limited to, Financial Services, Critical Manufacturing, and Government Facilities sectors.

It was first seen in mid-2021 when attackers use spam email campaigns as initial infection vectors for the delivery of the ransomware payload.

AvosLocker claims to directly handle ransom negotiations, as well as the publishing and hosting of exfiltrated victim data after their affiliates infect targets. As a result, AvosLocker indicators of compromise (IOCs) vary between indicators specific to AvosLocker malware and indicators specific to the individual affiliate responsible for the intrusion.

Like any other ransomware, AvosLocker encrypts files on a victim's machine and renames them with the [name] and .avos extension in Windows environment, on Linux environment is ".avoslinux".

Then attackers leave some type of message on the victim server and include a link to some type of payment or link to an AvosLocker .onion payment site.

Complete instruction you will have on how to pay the ransom, in some situations you may even get a call from the attacker instructing you on how to pay them money to retrieve your files.

Who is the target of ransomware attacks?

If you think you are not a victim if you do not work in one of the affected institutions, you are mistaken. Like all types of malware, the victim does not choose whether to be a corporation or a regular customer at home.

Our recommendation is to follow cyber security standards and policies if you are in a company, and if you are a regular user, be careful of the emails you receive because this is the most common entry for hackers for such attacks.

How to protect against AvosLocker Ransomware

First and foremost, follow the guidelines and policies if you're in the company. **To mitigate this type of threat, organizations need to**:

- **Implement a data recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physical, separate, segmented, and secure location, such as a hard drive, storage device, or the cloud.
- **Implement network segmentation** and maintain offline backups of data to ensure limited interruption to the organization.
- **Regularly back up data**, and password protected backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- **Use multi-factor authentication** where possible.
- **Install and regularly update antivirus software on all hosts**, and enable real-time detection. Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- **Focus on cyber security awareness and training**. Regularly provide users with training on information security principles and techniques as well as overall emerging cyber security risks and vulnerabilities (i.e., ransomware and phishing scams).

NIMBUSPWN VULNERABILITY

Analysis by: Dalibor Gašić

In April 2022, Microsoft 365 Defender Research team discovered a vulnerability named Nimbuspwn, where an attacker can gain escalation of privilege from local users with low capabilities to root access on multiple Linux desktop environments.

The “Nimbuspwn” vulnerability is recorded as CVE-2022-29799 (Directory Traversal) and CVE-2022-29800 (TOCTOU race conditions).

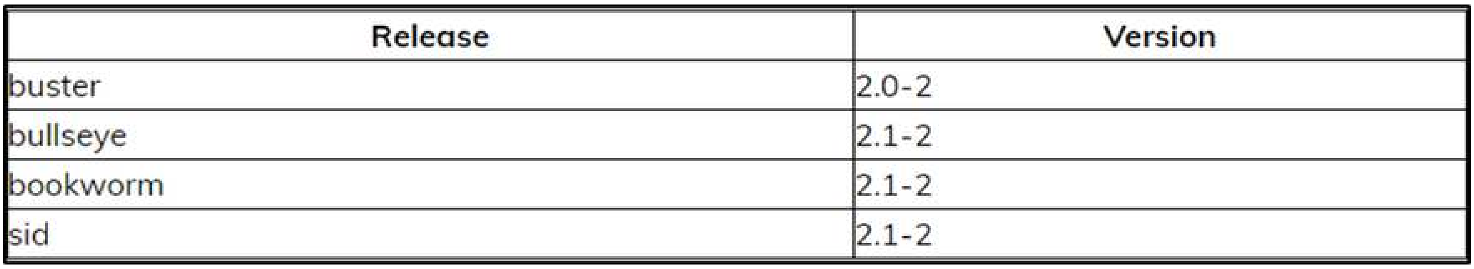
When these two vulnerabilities are linked together, they give the attacker root privileges and from there he can deploy other payloads, compromising Linux systems via arbitrary root code execution and potentially exposing compromised Linux environments to more advanced threats, including ransomware attacks to achieve greater impact on vulnerable devices.

Who is affected by this vulnerability?

According to research by the Microsoft Team, the vulnerability was found in networkd-dispatcher versions v2.0-2 and v2.1-2. For those who don't know, this service is responsible for systemd-networkd connection status changes.

It is similar to NetworkManager-dispatcher, but is much more limited in the types of events it supports due to the limited nature of systemd-networkd.

Reference: Detailed explanation for networkd-dispatcher.



Release	Version
buster	2.0-2
bullseye	2.1-2
bookworm	2.1-2
sid	2.1-2

How to check if you are you vulnerable

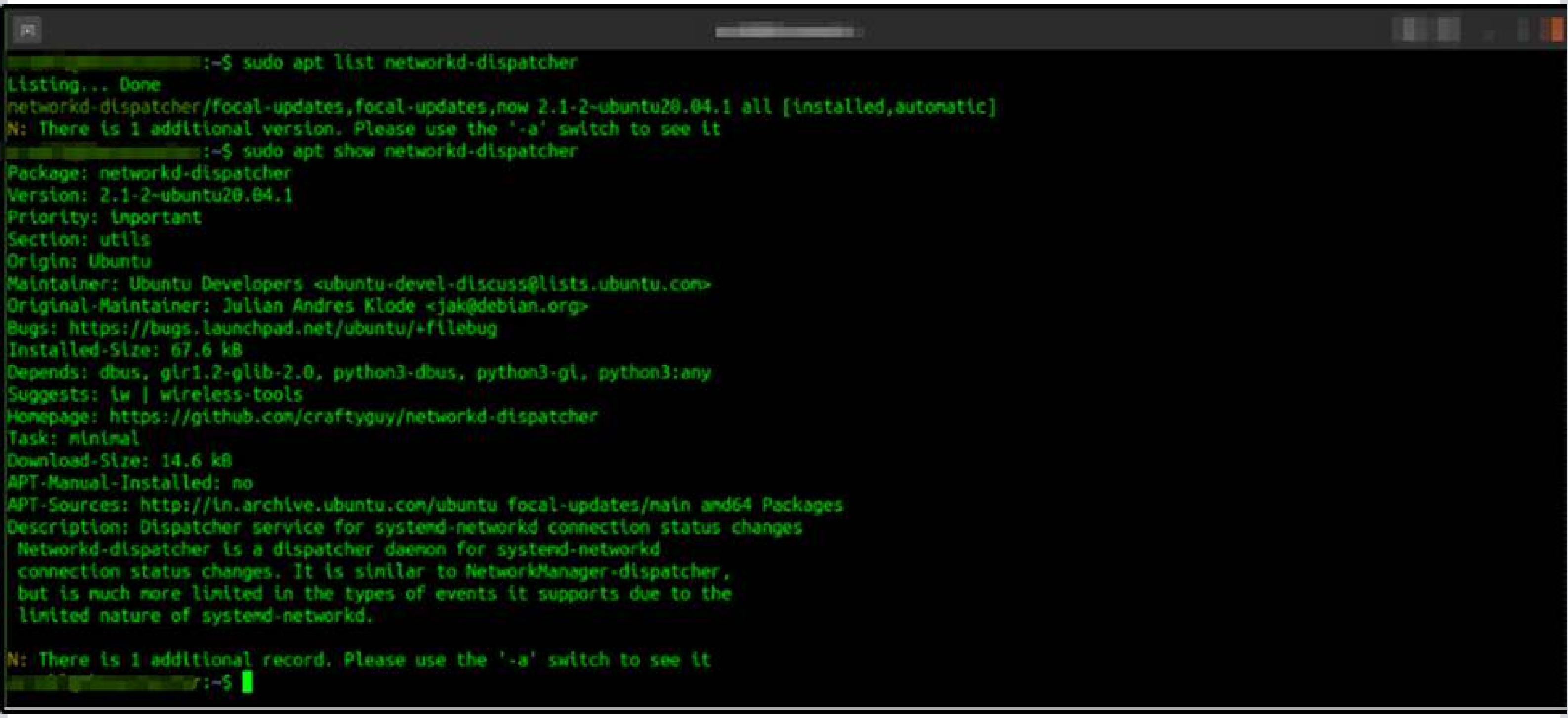
With these simple commands we can check on our Linux distribution whether this service exists and whether it is enabled, as well as which version it is.

Command: **$ sudo apt list networkd-dispatcher**

This command is enough to see the version information.

Command: **$ sudo apt show networkd-dispatcher**

This command will give your comprehensive information about the package.



```
[redacted]:~$ sudo apt list networkd-dispatcher
Listing... Done
networkd-dispatcher/focal-updates,focal-updates,now 2.1-2~ubuntu20.04.1 all [installed,automatic]
N: There is 1 additional version. Please use the '-a' switch to see it
[redacted]:~$ sudo apt show networkd-dispatcher
Package: networkd-dispatcher
Version: 2.1-2~ubuntu20.04.1
Priority: important
Section: utils
Origin: Ubuntu
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Original-Maintainer: Julian Andres Klode <jak@debian.org>
Bugs: https://bugs.launchpad.net/ubuntu/+filebug
Installed-Size: 67.6 kB
Depends: dbus, gir1.2-glib-2.0, python3-dbus, python3-gi, python3:any
Suggests: iw | wireless-tools
Homepage: https://github.com/craftyguy/networkd-dispatcher
Task: minimal
Download-Size: 14.6 kB
APT-Manual-Installed: no
APT-Sources: http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages
Description: Dispatcher service for systemd-networkd connection status changes
 Networkd-dispatcher is a dispatcher daemon for systemd-networkd
 connection status changes. It is similar to NetworkManager-dispatcher,
 but is much more limited in the types of events it supports due to the
 limited nature of systemd-networkd.

N: There is 1 additional record. Please use the '-a' switch to see it
[redacted]:~$
```

In the image below we can see an example of a vulnerable server as it's running v.2.1-2.

How to remediate this vulnerability

In case you have enabled service **networkd-dispatcher** with a vulnerable version on your Linux Distribution, we can recommend have few steps to fix this flaw:

- First, there are a few commands that we can use to update our system repositories: Command: **$ sudo apt update && sudo apt upgrade –y**
- Second, you need to upgrade your service if it is installed and enabled: Command: **$ sudo apt upgrade networkd-dispatcher**
- The last one, you can always remove this service if there is no fixed version: Command: **$ sudo remove networkd-dispatcher | sudo purge networkd-dispatcher**
- Find additional information here:
  - https://security-tracker.debian.org/tracker/source-package/networkd-dispatcher
  - https://ubuntu.com/security/CVE-2022-29799

Additionally, Microsoft recommended a “proactive vulnerability management approach” that identifies and mitigates previously unknown vulnerabilities. It is also recommended to install endpoint security solutions capable of detecting the directory traversal vulnerability required to complete the Nimbuspwn attack chain.

GOVERNMENT POLICY & REGULATION

Many of the toolkits, processes, strategies, and technologies that enter the commercial sectors come down from the U.S. government and its military branches.

Our experts, Rich Selvidge and Josh Allen have over 30 years of combined experience working firsthand for U.S. Cyber Command, DoD, Special Operations, and Defense Industries to bring their analysis on the latest regulations, departments, and techniques that you should need to know.

In this month's issue we cover:

- Operational Continuity-Cyber Incident (OCCI)

The Cybersecurity Working Group (CWG) of the Healthcare and Public Health Sector Coordinating Council (HSCC) has produced a checklist to assist healthcare professionals and executives in maintaining operational continuity while recovering from a significant breach

HSCC had issued advice on medical device vulnerability communications just a week before.

The Operational Continuity-Cyber Incident (OCCI) checklist can help healthcare organizations **maintain business continuity even if their systems are down for an extended period of time,** according to the HSCC.

The checklist, which was developed by the HSCC's CWG's Incident Response/Business Continuity (IRBC) Task Group, is intended to be a live document that may be updated depending on stakeholder comments and experience.

"*As the IRBC Task Group was forming, it was clear that geopolitical tensions arising from the Ukraine-Russia conflict were posing a greater threat to the health sector, necessitating increased awareness and immediate preparations against potential disruptions in health care delivery,*" the document began.

"*As a result, the HSCC created this tactical checklist with an accelerated development cycle through the IRBC TG to anticipate the potential for an extended outage in the event of direct cyber-attacks or collateral fallout and get it into the hands of our stakeholders as soon as possible*," says the HSCC.

The Cybersecurity and Infrastructure Security Agency (CISA) raised the alarm about Russian state-sponsored cyber-attacks once again in late April. Patching all systems, securing Remote Desktop Protocol (RDP), and implementing multifactor authentication are all recommendations made by CISA for critical infrastructure.

Even if there **isn't a direct hack on US healthcare companies**, the American Hospital Association (AHA) has warned that **Russian-deployed malware may cause collateral harm**.

With geopolitical tensions in mind, the HSCC's handbook addresses the risk of a "prolonged major disruption," which it defines as an event that might jeopardize patient safety and clinical operations.

The HSCC Handbook is divided into sections depending on distinct organizational functions. An "**incident commander**," for example, should be named to offer "overall strategic guidance on all site-specific reaction operations and activities."

The incident commander should first **determine the breadth of the issue and set up a cadence and procedure for interacting with IT and cyber security teams**, according to HSCC. Activate downtime plans and engage with partner companies about downstream consequences within the first 12 hours, according to the checklist.

Meanwhile, the incident commander's designated medical-technical specialist should consult with risk management and legal specialists to determine suitable reaction measures and compliance activities.

According to the checklist, the public information officer acts as "*a conduit for information to internal and external stakeholders, including site workers, visitors and families, and the news media*."

Briefings should be given to the public information officer, and internal and external communications, as well as crisis communication strategies, should be developed. The officer should also work with public relations (PR) specialists and offer media outlets with information.

Other recommended positions for performing different recovery activities were a liaison, a safety officer, a finance section head, and a logistics section chief.

The responsibilities were responsible for meeting recovery time goals, communicating with patients, employees, and visitors, and ensuring that food and drink were accessible.

HIPAA mandates the implementation of a cyber incident response plan, but with the current increase in cyberattacks, businesses should be even more prepared to put their plans into action.

Even in the midst of a cyber attack, businesses may retain business continuity by thinking through each part of incident response and recovery, as well as identifying roles and responsibilities.

What you should do:

The Cybersecurity and Infrastructure Security Agency (CISA) raised the alarm about Russian state-sponsored cyber-attacks once again in late April.

- **Patching all systems**, securing Remote Desktop Protocol (RDP), and implementing multifactor authentication are all recommendations made by CISA for critical infrastructure.
- **Conduct a Risk Assessment**, know what your exposure actually is by bringing in a third party assessor to validate your posture.
- **Test your business continuity plan** (BCP) to ensure the process your company undergoes will create a prevention and recovery system from potential threats such as natural disasters or cyber-attacks.
- Test your backups.

To ensure you have a proven process for protecting your company's data, you'll want to know this information:

Know your data

- What's the nature of the data that drives your company?
- What is the level of importance for that data?
- Where does it reside?
- How is it secured?
- How is it protected?
- Who has access to it?

Know your applications

- What data sits in each application?
- Is the application on a physical server or a virtual server?
- Are there key requirements for any of the applications?
- Who uses the application and what data do they have access to?
- How are the applications protected?
- Who are the application business owners?

HEALTHCARE SECURITY

Get thought leadership analysis and actionable steps you can take to better secure your organization from cyber attacks. Led by our healthcare security expert, Rich Selvidge, we'll get you up to date on the latest breaches and regulations in healthcare.

In this month's issue we cover:

- Adaptive Health Integrations Breach
- Zero-Day Vulnerabilities On The Rise

("AHI") reported a data breach that **affected more than 510,574 people** in one of the greatest data breaches in recent months. AHI notified the federal officials of the **breach on April 11, 2022**, and began issuing out data breach notifications to people whose personal information had been exposed.

While the organization has not yet made the detailed information on how it was hacked public, it is critical that you educate yourself about the hazards of data breaches and take the necessary steps to reduce the risk of fraud or identity theft.

Given the recent nature of the AHI hack, few facts concerning the event have been released. Adaptive Health Integrations, however, realized that an **unauthorized entity gained access to the firm's computer system on or around October 17, 2021**, according to an official filing by the company.

AHI initiated an inquiry into the breach after learning about it, in order to discover more about what caused it and whether any consumer information had been exposed.

AHI announced **on February 23, 2022, that people's personal data had been exposed**. Adaptive Health Integrations began notifying all impacted parties of a data incident on or around April 11, 2022.

ADAPTIVE HEALTH INTEGRATIONS

Analysis by: Rich Selvidge, CISSP

Adaptive Health Integrations, based in Williston, North Dakota, offers labs, healthcare firms, and doctors' offices a variety of billing and software support services. MedScan Laboratory, Inc. and Adaptive Health Integrations are partners.

Williston, ND, Atlanta, GA, and Houston, TX are the locations of Medscan Laboratory. Medscan Laboratory employs 164 employees and has an annual revenue of over $30 million.

Protected health information data breaches are different from data breaches involving Social Security numbers and bank account information.

According to Experian, a credit reporting bureau, **the average cost per record, of repairing a healthcare data breach is $13,500**.

A healthcare data breach primarily poses the risk of someone using your personal information to receive medical treatment in your name.

This might result in you receiving medical fees for operations you never had done, but it is also possible that your medical record will contain false information given by the criminal who stole your identity.

Given this fact, it is critical for people whose protected health information has been exposed as a consequence of a data breach to take precautions.

1. Gather Evidence And File A Report

After a healthcare data breach, the first thing you should do is gather any evidence that your protected health information has been taken. This includes any bogus medical bills as well as the company's data breach notice. In addition, you should file an Identity Theft Report with the Federal Trade Commission.

2. Go Over Your Medical Records That Are Currently On File

This is the most difficult, but also the most crucial, phase. All of your medical records should be gathered and reviewed for correctness. Keep an eye out for any therapies that you have never heard of before. It is also a good idea to double-check the addresses and phone numbers on file.

3. All Errors Must Be Fixed

If you detect an error in your medical records, ask the physician to rectify it. **The last thing you want is for your medical records to include inaccuracies**, such as a medicine allergy that has gone unnoticed.

ZERO-DAYS ON THE RISE

Analysis by: Rich Selvidge, CISSP

According to Mandiant Threat Intelligence's newest research, there were a record number of zero-day vulnerabilities in 2021. In 2021, the company found eighty exploited zero-days, compared to only 30 in 2020. **Threat actors favored zero-day vulnerabilities in Google, Microsoft, and Apple products** the most, illustrating the businesses' attractiveness.

The Health Sector Cybersecurity Coordination Center (HC3) of the Department of Health and Human Services (HHS) released a threat brief in late 2021 describing the dangers and mitigation methods connected with zero-day attacks on the healthcare sector.

Mandiant discovered about two hundred zero-day vulnerabilities between 2012 and 2021. Mandiant only saw two zero-days in 2012. Zero-day exploits, on the other hand, have exploded in popularity in recent years across all industries.

The rise in cloud hosting, mobile, and internet of things (IoT) technologies, according to Mandiant, has increased the complexity of internet-connected devices.

Researchers said that as the variety of software options grew over time, so did the number of vulnerabilities.

The expansion of the exploit broker marketplace also likely contributes to this trend," the paper stated, "with more resources being diverted toward zero-day research and development, both by commercial organizations and researchers, as well as threat groups."

"Finally, improved defenses are likely allowing defenders to identify more zero-day exploitation now than in prior years, and more firms have tightened security practices to limit breaches via other routes," says the report.

Zero-day vulnerabilities in the healthcare records application OpenClinic revealed patient test results in August 2020. After the developers failed to respond to allegations of four zero-day vulnerabilities, users were advised to discontinue using the open-source application. **Unauthorized actors were able to get files containing protected health information** by submitting a request (PHI).

Pneumatic tube systems used by hospitals to carry bloodwork, test samples, and drugs were disrupted by the zero-day vulnerability known as "**PwnedPiper**" in August 2021.

The attackers were able to take advantage of weaknesses in the control panel software, allowing unauthenticated and unencrypted firmware changes.

Because healthcare data is a high-value target, it may be particularly vulnerable to zero-day assaults. Patching is also the most effective mitigating strategy, although it might be difficult to do on outdated systems and medical IoT equipment.

State-sponsored espionage outfits continue to be the leading threat actors using zero-day vulnerabilities, according to Mandiant. Threat actors that profit on zero-day exploits, on the other hand, are on the rise.

Mandiant discovered a **large number of suspected Chinese cyber espionage groups using zero-day exploits in 2021**. According to the research, China exploited more zero-day vulnerabilities than any other country between 2012 and 2021.

"We believe that significant campaigns based on zero-day exploitation are becoming more accessible to a broader range of state-sponsored and financially motivated actors," according to the report, "including as a result of the proliferation of vendors selling exploits and sophisticated ransomware operations potentially developing custom exploits."

ZERO-DAYS ON THE RISE

Analysis by: Rich Selvidge, CISSP

The significant growth in **zero-day vulnerability exploitation, especially in 2021, widens the risk portfolio for businesses in practically every industrial area and region**." While exploitation peaked in 2021, there are signs that the rate of new zero-day exploitation declined in the second half of the year; still, zero-day exploitation continues at a high rate in comparison to prior years."

What you can do:

- When possible, organizations should **look for automated solutions** to lower costs, enhance efficiency, and improve the reliability of monitoring security-related information. Security is implemented through a combination of people, processes, and technology.
- Organizations should **create a defense plan** and prioritize addressing known vulnerabilities, according to the researchers.
- **Develop a continuous monitoring program** to reduce the window of opportunity that bad actors can take advantage of.

CRYPTO & BLOCKCHAIN

With the rise of cryptocurrency came the seemingly endless applications of blockchain technologies. One of the most interesting applications is in the cyber security space.

Our expert, Ken Thomas, brings forward his analysis on current trends in the crypto and blockchain community and attempts to demystify and explain its uses well beyond the marketing buzzwords.

In this month's issue we cover:

- State Sponsored APT Targeting Crypto
- Instagram Phishing Attacks Costs $1M

STATE SPONSORED APT TARGETS CRYPTO

Analysis by: Ken Thomas

On April 18th, 2022 the FBI, Department of Treasury, and CISA (Cybersecurity & Infrastructure Security Agency) issued a joint Cyber security Advisory alert (AA22-108A) for newly observed APT campaigns actively targeting crypto currency users, decentralized finance (defi) protocols, centralized exchanges, and holders of large amounts of valuable tokens.

Social engineering is the primary tactic used to incentivize victims to download malicious applications that contain weaponized binaries intent on separating users from their crypto holdings and weakening the security of targeted environments.

Once infected the attackers then use the malicious application to move laterally within the network, propagating malware to any susceptible hosts, stealing users' private keys, and performing other malicious command/control activities.

The malware associated with these attacks is known as ‘TraderTraitor’ and has been observed in use by North Korean state-sponsored actors since 2020.

CISA has identified the TTP's (tools, techniques, procedures) associated with the observed attacks as part of HIDDEN_COBRA, Lazarus Group/APT38 campaigns. In previous campaigns, The Lazarus Group has targeted numerous institutions within the energy, government, finance, and technology via AppleJeus malware.

In alert (AA21-048A) "AppleJeus: Analysis of North Korea's Cryptocurrency Malware" updated on April 15th, 2021 CISA reports:

"Since January 2020, the threat actors have targeted these sectors in the following countries: Argentina, Australia, Belgium, Brazil, Canada, China, Denmark, Estonia, Germany, Hong Kong, Hungary, India, Ireland, Israel, Italy, Japan, Luxembourg, Malta, the Netherlands, New Zealand, Poland, Russia, Saudi Arabia, Singapore, Slovenia, South Korea, Spain, Sweden, Turkey, the United Kingdom, and the United States."

TraderTraitor is the term given by CISA to malware written in javascript environments such as node.js featuring modern looking websites and Electron framework interfaces.

These malicious binaries are often derived from open source projects and claim to be software useful to traders such as price prediction markets, artificial intelligence platforms, and cryptocurrency portfolio management.

Targets include employees within cryptocurrency companies, especially those working in systems administration, site reliability engineers, IT and/or software development.

TraderTraitor malware will **include malicious javascript intended to appear as a benign update function** that in fact download and execute's attacker controlled payloads. The update functions will typically perform an HTTP POST request to a malicious script or web endpoint ex: '/update/' hosted on the attacker controlled domain.

Payloads include custom variants of MacOS, and Windows Remote Access Trojan (RAT) software 'Manuscrypt' which can collect system information, execute malicious commands, and download additional malicious payloads.

Users are advised to take an 'in depth' approach to security, including:

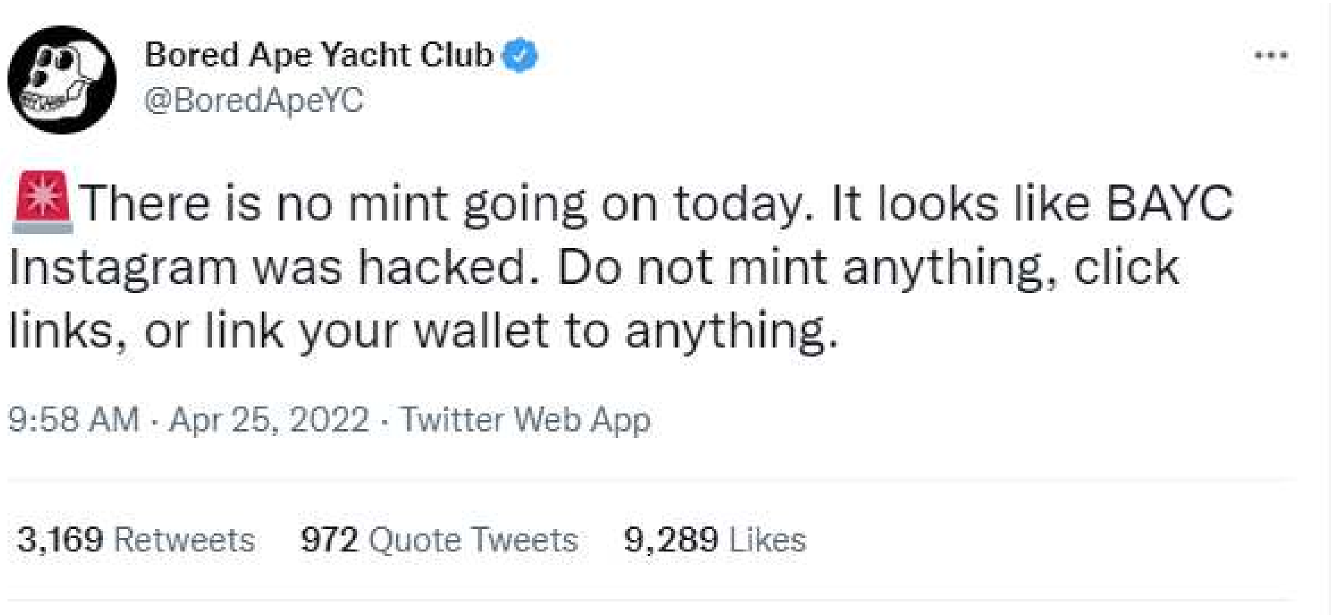
- Adapt the principle of least access
- Enforce multi-factor access
- Segregate network access
- Setup endpoint protection and device management
- Develop a vulnerability management program
- Implement strong email protection featuring malware engine, attachment scanning, and phish reporting.
- Develop and educate employees on popular techniques
- Create an incident response plan

$1M LOST IN INSTAGRAM PHISH

Analysis by: Ken Thomas

Yugalabs project BAYC (Bored Ape Yacht Club) recently found itself the victim of a phishing attack resulting in **over $1 million in losses of tokens and valuable NFT's**. Users were directed to malicious domain 'yugalabs dot land' from the BAYC Instagram and encouraged to connect their wallets.

The message posted to Twitter by @BoredApeYC on April 25th, 2022:



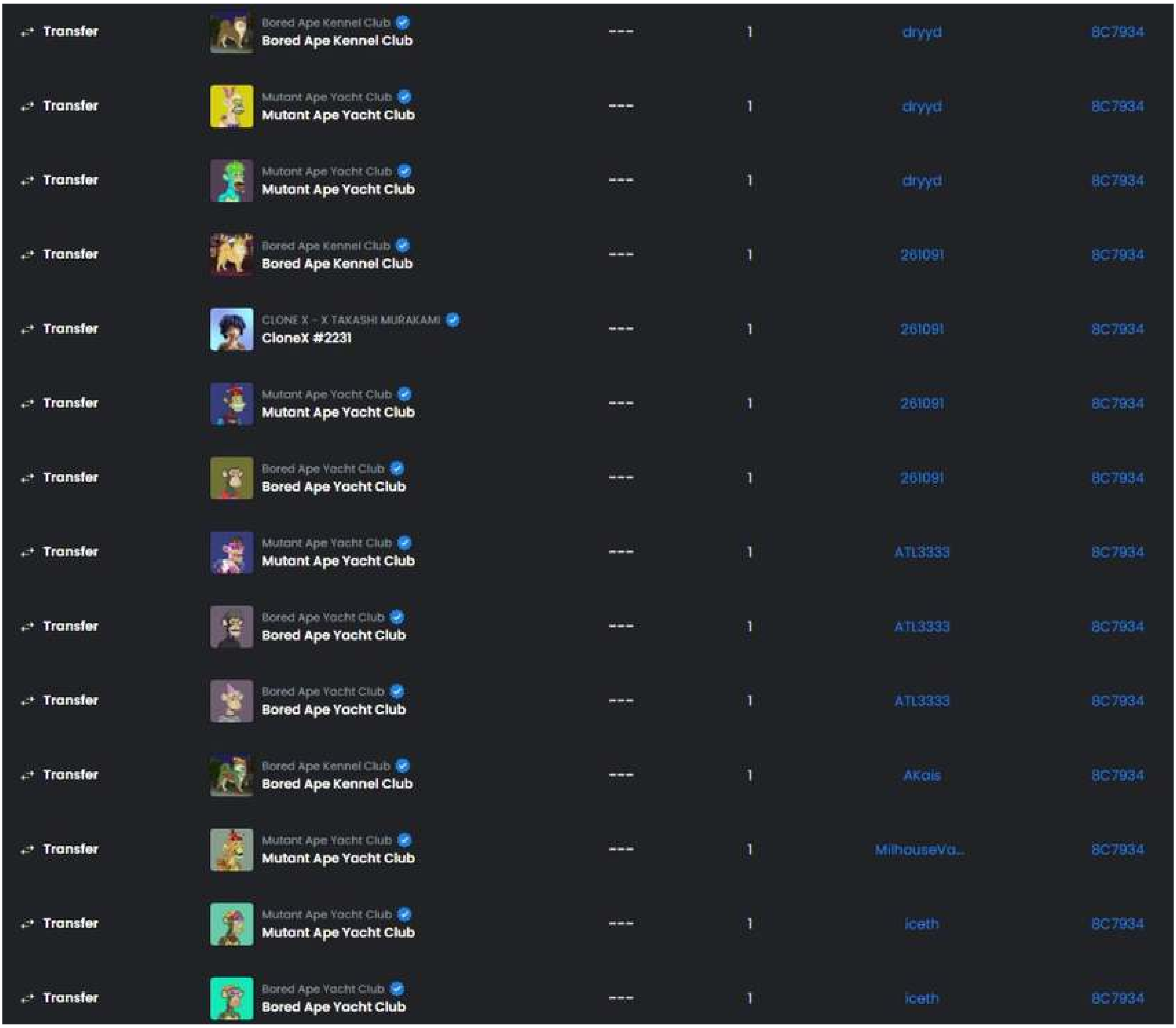
Bored Ape Yacht Club
@BoredApeYC

🚨There is no mint going on today. It looks like BAYC Instagram was hacked. Do not mint anything, click links, or link your wallet to anything.

9:58 AM · Apr 25, 2022 · Twitter Web App

3,169 Retweets   972 Quote Tweets   9,289 Likes

However, this may have come too late as indicated by @dingdingETH on the same thread "expensive day to reimburse those affected"



Transfer	Bored Ape Kennel Club Bored Ape Kennel Club	---	1	dryyd	8C7934
Transfer	Mutant Ape Yacht Club Mutant Ape Yacht Club	---	1	dryyd	8C7934
Transfer	Mutant Ape Yacht Club Mutant Ape Yacht Club	---	1	dryyd	8C7934
Transfer	Bored Ape Kennel Club Bored Ape Kennel Club	---	1	261091	8C7934
Transfer	CLONE X - X TAKASHI MURAKAMI CloneX #2231	---	1	261091	8C7934
Transfer	Mutant Ape Yacht Club Mutant Ape Yacht Club	---	1	261091	8C7934
Transfer	Bored Ape Yacht Club Bored Ape Yacht Club	---	1	261091	8C7934
Transfer	Mutant Ape Yacht Club Mutant Ape Yacht Club	---	1	ATL3333	8C7934
Transfer	Bored Ape Yacht Club Bored Ape Yacht Club	---	1	ATL3333	8C7934
Transfer	Bored Ape Yacht Club Bored Ape Yacht Club	---	1	ATL3333	8C7934
Transfer	Bored Ape Kennel Club Bored Ape Kennel Club	---	1	AKais	8C7934
Transfer	Mutant Ape Yacht Club Mutant Ape Yacht Club	---	1	MilhouseVa...	8C7934
Transfer	Mutant Ape Yacht Club Mutant Ape Yacht Club	---	1	iceth	8C7934
Transfer	Bored Ape Yacht Club Bored Ape Yacht Club	---	1	iceth	8C7934

The vector for the attack is still unknown at this time as BAYC's Instagram is reported to have had two-factor authentication enabled. In a post to Twitter @BoredApeYC states on April 25th 2022 "At the time of the hack, **two-factor authentication was enabled and security surrounding the IG account followed best practices**.

Other security researchers have suggested YugaLabs could have been **victim of a reverse proxy attack**, targeting the staff of YugaLabs employees who had access to the company's Instagram account.

In traditional phishing attacks malicious content is served to a targeted user via an attacker controlled mechanism (website, email, etc).

With a reverse proxy **the attacker is able to insert themselves in between valid server communications to / from the targeted user** originating from an attacker controlled domain.

Metacert CEO Paul Walsh suggest “How the Bored Ape Yacht Club was probably compromised with a reverse-proxy phishing attack” on April 25th, 2022 that YugaLabs was potentially targeted via automated phishing software like Modlishka (Polish for Mantis).

What you can do:

Users should verify all URL’s via https://urlscan.io and https://virustotal.com prior to connecting their wallets to new decentralized applications (dapps) since attackers will tend to re-use content from other successful crypto theft campaigns.

Additionally, users can revoke dapp connectivity via https://revoke.cash.

While crypto users are strongly encouraged to engage in best security practices, it is uncertain where responsibility for this hack lies and if YugaLabs will compensate affected token holders.

MEET OUR EXPERTS

Jason Firch, MBA

Chief Executive Officer

Jason is a veteran IT operations manager and digital marketer with a decade of experience. He is also the co-founder of PurpleSec and services as both the CEO and CMO.

Throughout his career, Jason has developed, deployed and evaluated successful digital, inbound, paid, social media and content marketing initiatives in technology industries.

Jason holds both an MBA and BA with a focus on marketing from Bloomsburg University of Pennsylvania. He is a recipient of multiple sales awards and has been published in an international business journal. When he's not studying for his CISSP or contributing to the PurpleSec blog, you'll find Jason helping nonprofits with their online marketing.

MEET OUR EXPERTS

Seth Kimmel, OSCP

Chief Technology Officer

Seth is an accomplished cyber security professional with 10 years of proven experience leading teams and projects to successful completion for an enterprise company with over 700 employees. Seth is the co-founder and Chief Technology Officer of PurpleSec, as well as a military veteran having served 6 years in the United States Marine Corps.

Seth holds both a BS in Security Risk Analysis – Information and Cyber Security, from Pennsylvania State University, and the coveted Offensive Security Certified Professional (OSCP) certification. When Seth isn't building systems to defend against cyber attacks, you'll find him outdoors spending time with his Golden Retriever, Murphy, or wrapped up in a Hardcore History podcast.

MEET OUR EXPERTS

Rich Selvidge, CISSP

Chief Information Security Officer

Rich Selvidge is the CISO at PurpleSec with over 21 years of information technology and security risk management experience. Prior to joining PurpleSec, he was the Manager of Information Security Governance and Compliance at American Automobile Association national office.

Working at various offices within the Department of Defense, Rich was responsible for teams of information security professionals who provided information security risk prevention and deterrence services, globally.

He was simultaneously accountable for all information security controls outside of the United States within the DoD Research community covering forty-eight countries.

MEET OUR EXPERTS

Josh Allen

Chief Product Officer

Joshua is a diversely-skilled cyber security professional with 10 years of Department of Defense cyber security experience. He currently serves as PurpleSec's Chief Product Officer responsible for creating and developing bleeding edge technologies and processes to service SMB and Enterprise clients.

Josh has recently served as a team lead for a Secure Operations (SOC) environment supervising a team in a fast-paced cloud security as a service company. Joshua’s skillsets include enterprise architecture hardening, penetration testing, web application firewall management, network security, data privacy and classification, and enterprise risk assessment.

MEET OUR EXPERTS

Michael Swanagan, CISSP, CISA, CISM

Senior Security Advisor

Michael is an Information Security Professional with 13 years of proven experience. He has experience leading and supporting security projects and initiatives in the healthcare, finance, and advertising industry. Michael is also an expert in helping SMBs develop effective security strategies.

He specializes in Data Loss Prevention, implementing and supporting DLP in medium and large global organizations. His expertise lies in providing a DLP road map to protect your confidential data at the endpoint, in transit or network, or data at rest.

Michael is also the editor of PurpleSec, ensuring the technical accuracy of all content published online.

Kenneth Thomas

Senior Security Advisor

Kenneth Thomas is a Corporate Security Professional for the Oil & Gas industry with over 10 years of cyber security experience and the founder of Telegram web3 community ‘**meefs NFT Corner**’.

Kenneth specializes in enterprise cloud security, blockchain development, and community building. Kenneth has a passion for artificial intelligence, creating bespoke meta verse experiences, and cloud architecture.

Dalibor Gašić

Senior Security Engineer

Dalibor is a Senior Security Engineer with experience in penetration testing, and an active Bug Bounty hunter on platforms such as HackerOne, Bugcrowd, and Integrity. In the past, he worked as a Security Consultant for several companies, where he gave recommendations and advice on how to protect companies from cyber attacks.

He also served 8 years in the Ministry of Internal Affairs in the Department of Cyber Security in Serbia.