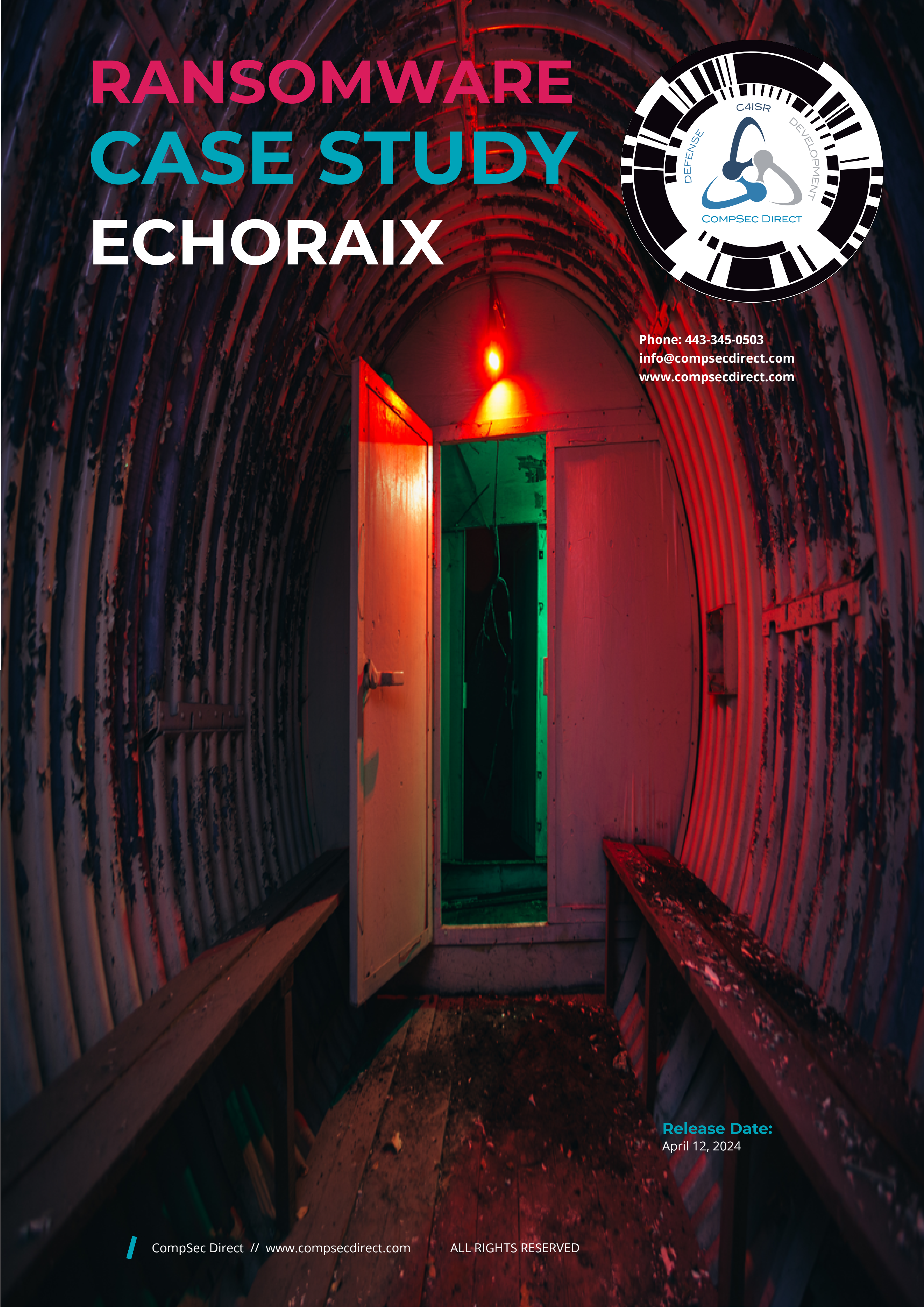


RANSOMWARE CASE STUDY

ECHORAIX

Phone: 443-345-0503
info@compsecdirect.com
www.compsecdirect.com

Release Date:
April 12, 2024

José Fernández
President

THANK YOU
FOR VIEWING THIS STUDY

Ransomware has changed the game. Companies must take perimeter-defense seriously. Attackers have the advantage of time, and the SMB market generally has infective or non-existent cyber security policies, planning and procedures to handle digital threats. This Ransomware group was overshadowed in Dec of 2021 by more concerning vulnerabilities against products with more market presence and to our surprise; little to no reporting was done to capture what this group accomplished at the end of 2021.

We continued to observe some of the infrastructure that we identified while performing incident response for a victim and felt it was necessary to ensure that others knew about this group since lack of awareness of issues within InfoSec generally translates to obliviousness of risks within SMB. We hope this report helps others and would encourage you to reach out with any comments or concerns related to findings we shared within this report.

151 Calle San Francisco
Suite 200
San Juan, PR, 00901

Phone: 443-345-0503
E-mail: info@compsecdirect.com
www.compsecdirect.com

Content: José Fernández
Design: María de los Ángeles-Pagán
Marketing and press: Ivette Rodriguez
Revisions: Oscar Fuentes

CONTENT

AS I.T. CONTINUES TO FAIL US, THINK...

THEY DON'T GET "IT"

CompSec Direct provided initial Incident Response efforts for a customer within the entertainment industry. This customer is in the SMB market and we are optimistic that the findings in this report can help others.

SMBs generally have lax security configurations. Most cannot afford to have dedicated staff to provide digital security and often assume that the "I.T. person" or company they use for I.T. services will ensure they are resilient against security threats, while also keeping overhead costs down. Over time, I.T. is simply pressured to maintain availability, ease of access, and use of the systems they help maintain. In some cases, when I.T. attempts to improve the security posture for a client, they don't get "IT" right the first time and the business owners become furious as this impacts business operations. Although overlap in functions may exists between I.T. and cyber-security; one gets "IT" and the other doesn't get "IT".

CompSec Direct provided guidance, recommendations, and action items for the customer to follow to recover from this attack.

QUICK FACTS

... FOR THOSE UNFAMILIAR WITH ECHORAIX

eCHoraix has been around since 2019

The group has impacted the affordable and user-friendly NAS devices from Taiwanese manufacturer QNAP. In the past, the group developed ransomware code and made a programming mistake which made recovery of encrypted files possible.

Low-Cost NAS devices are at risk

Companies such as QNAP and Synology have created significant market adoption within the NAS ecosystem of devices. Market adoption of low-cost IoT devices provides strong metrics for attackers to develop capabilities against certain product lines. eChoraix has ransomed thousands of victims, and in some cases individuals that paid up did not get working recovery keys to decrypt their files.

echoraix is similar to qnapcrypt & suncrypt

Reports from 3rd parties have analyzed previous ransomware activity related to these groups. It is possible to analyze ransomware samples using online services & our disassociated range: Kleared4. Threat actors piece-meal, & steal code snippets; like digital jawas.

Ransomware sample within container

This group has x86 and ARM versions of ransomware. We have an easy-to-use docker container which analysts can use to analyze certain Linux malware, including the x86 sample from eCHoraix. Please check our social media sites for links, instructions and videos related to the use of this container.

Follow us on LinkedIn: compsec-direct and Facebook CompSecDirect

EXECUTIVE SUMMARY

IMPACT FACTS

Vulnerability Old firmware version. The group may have utilized any number of QNAP exploits due to the firmware version being from early 2019 despite being Dec 2021 when the event occurred.

Initial Access Exposed TCP80/443. We believe CVE-2019-7193 was used to access the device over the exposed web-interface.

Behavioral activity The system logs suggest local user accounts were used in what seems as a manual non-automated process of testing accounts, meaning that a person logged to familiarize themselves with the device and contents.

Persistence A malicious service is deployed to the victim box called QS118System. wget downloads and executes both x86 and ARM samples within a screen session

Impact Victims /share/ mounts are targeted by default, and master decryption key for this version is not avaiable yet leaving thousands of victims worldwide.

EXECUTIVE SUMMARY
CONDENSED FACTS

Staff Identified Ransomware

Staff at the victim site identified the issue during the winter holidays. The ransomware leaves decryption instructions that they were not comfortable doing themselves due to unfamiliarity with Tor.

Assistance to restore availability

CompSec Direct was contacted to assist the victim with this situation. We ensured that the owner understood what to do next and how to reduce the likelihood of a future attack.

WIFI Router enabled remote access

The existing wifi router in the victim company had uPnP enabled. This allowed a fresh QNAP device to use factory settings to enable public remote access to the device by exposing itself on well known ports.

The device was recently installed

An IT contractor had recently replaced a similar QNAP unit due to electrical problems. The contractor is partially to blame for the breach by not performing a firmware upgrade.

QNAP security was contacted

We shared technical information with QNAP regarding a persistence mechanism that appeared pre-existing within QNAP devices. QNAP answered all of our questions to help deconflict reporting and secondary actions.

We provided strategic advisory

CompSec Direct provided the initial strategic advisory needed to help the victim company coordinate and mitigate the effects of malicious activity from eCHoraix.

THIS COULD HAVE

BEEN AVOIDED

Proactive-Defenses

Scanning, monitoring, testing your Infrastructure before a problem occurs.

Requires outsourcing and Independent evaluations.

Perimeter Scanning

Using internal scanning helps identify your IT eco-system. External scanning would have identified how this eco-system is accessible remotely.

Continuous Monitoring

The IT eco-system outnumbers your staff. Without custom fitted monitoring solutions, your staff will not be able to effectively respond to incidents.

Testing

Mature organizations will test disaster recovery scenarios regularly towards recovery objective points. As more test are performed, logistical and technical gaps become reduced and refined. In house staff is already dedicated towards availability, not resilience.

OUR MAIN AREAS OF EXPERTISE RELATED TO THE INCIDENT

WE ENCOURAGE YOU TO REACH OUT AND CONTACT US ABOUT THESE SERVICES

Malware analysis

We analyzed the binary, and performed pinpointed research during the incident. This information was used to help defend the network. Go binaries are more difficult to analyze. We used containers on Kleared4 to test the malware, thousands of times.

Ransomware Protection

We harden systems, accounts, and services to reduce the likelyhood of a of sucessfull ransomware campaign on your networks. Our service includes proven configurations to help keep your networks safe.

Hunt as a Service

Our experience sets us apart from “leaders” in cyber that peddle expensive, unreliable software as resellers; not as developers of the products themselves. We use our custom Kleared4 Edge devices fly-away kits to perform Hunt in your networks.

Incident Response

Timing is critical, and once a breach is detected; you need to call experts to reduce the impact this will have on your staff. Having pre-established relationships with multiple response vendors reduces start paperwork, and enables vendors to work on the problem; your breach, and not your procurement process.

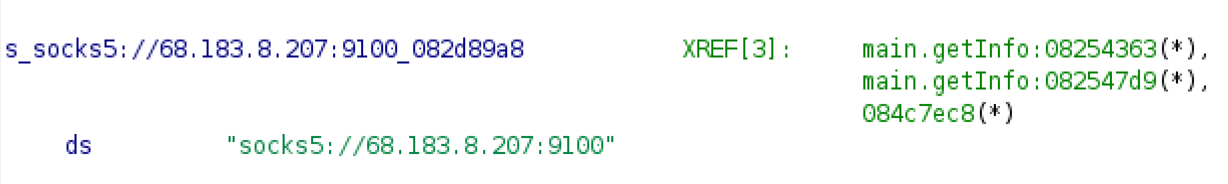
TECHNICAL ANALYSIS

CONDENSED FACTS AND TIMELINE

- #RANSOMWARE: GO BINARY: 386
2342E6A53DB8F97A676A6C6AB74CB10E5679D609
#RANSOMWARE: GO BINARY: ARM
F27F4898E0C08CD8D4DDEC1DDFCEB5BF ARM

- #USES QWATCHDOGD TO COMMUNICATE OVER TOR
774E9DC818EA03E63CB8226517A1CB5AB2639930 QWATCHDOGD

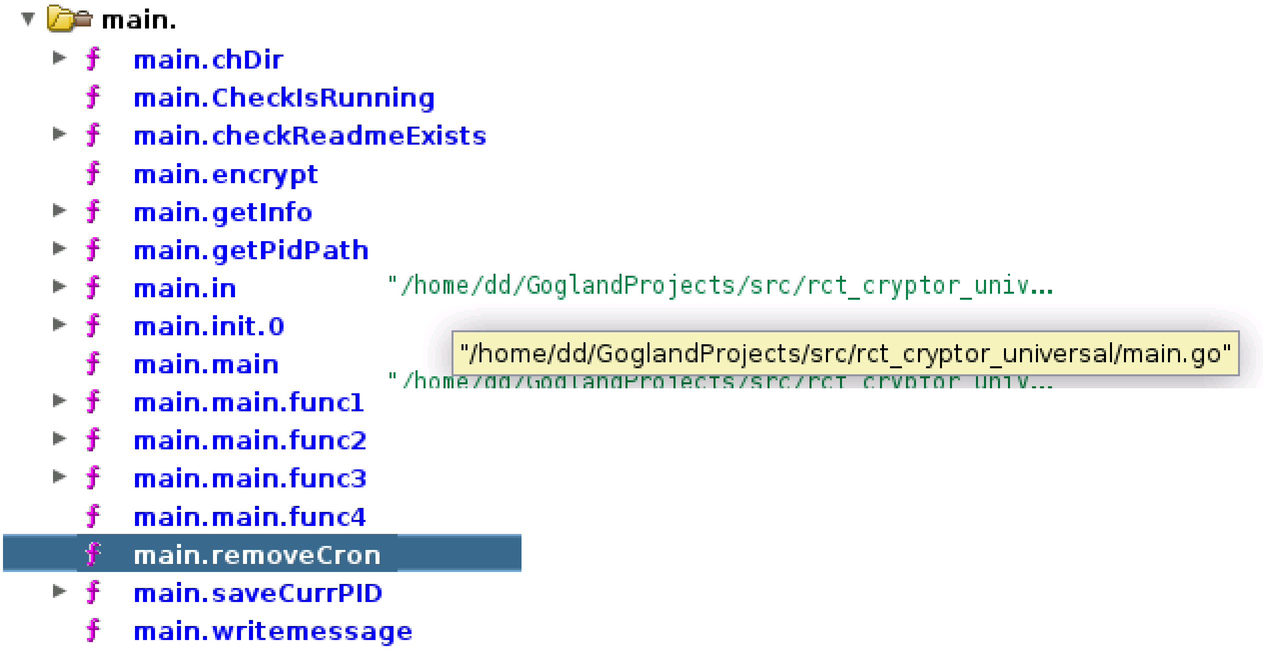
- #PERSISTENCE MIMICS EXISTING SERVICES IN /ETC/RCS.D/
/SHARE/CACHEDEV1_DATA/.QPKG/SYSTEM/SYSTEM.INIT+
/ETC/RCS.D/QS118SYSTEM



```
s_socks5://68.183.8.207:9100_082d89a8          XREF[3]:     main.getInfo:08254363(*),
                                                            main.getInfo:082547d9(*),
                                                            084c7ec8(*)
    ds          "socks5://68.183.8.207:9100"
```

- qWatchdog binary uploaded to VT since 2017, “re-analyzing” determined it also works as a tor client.

- QNAP does not explain how backend services work in an open manner; therefore all the backend scripts look malicious at first glance.



```
▼ main.
  ► ƒ main.chDir
    ƒ main.CheckIsRunning
  ► ƒ main.checkReadmeExists
    ƒ main.encrypt
  ► ƒ main.getInfo
  ► ƒ main.getPidPath
  ► ƒ main.in              "/home/dd/GoglandProjects/src/rct_cryptor_univ...
  ► ƒ main.init.0
    ƒ main.main            "/home/dd/GoglandProjects/src/rct_cryptor_univ...
  ► ƒ main.main.func1
  ► ƒ main.main.func2
  ► ƒ main.main.func3
    ƒ main.main.func4
    ƒ main.removeCron
  ► ƒ main.saveCurrPID
    ƒ main.writemessage
```

"/home/dd/GoglandProjects/src/rct_cryptor_universal/main.go"

echoraix was active while log4j occured

The group went largely unnoticed by other researchers that were actively remediating log4j threats.

This provided ample time for them to ransom victims.

Few malware samples were recovered for analysis; we captured two using our expertise in Linux systems.

DATA BREACH, RANSOMWARE, AND UNCERTAINTY

Summary of events from Dec, 2021 to Mar, 2022

- QNAP FAILS DUE TO UNSTABLE POWER IN PUERTO RICO. A REPLACEMENT IS FIELDED BY A 3RD PARTY.

> Power failures from brownouts damaged original NAS
> The Wireless router has UPNP enabled.
> The Firmware version of replacement NAS was from 2019.

- COMPSEC DIRECT IDENTIFIED THAT THE 3RD PARTY DID NOT UPGRADE THE FIRMWARE. THIS RESULTED IN EXPLOITATION AT LEAST ONE WEEK AFTER THE DEVICE WAS REPLACED, DURING THE HOLIDAYS.

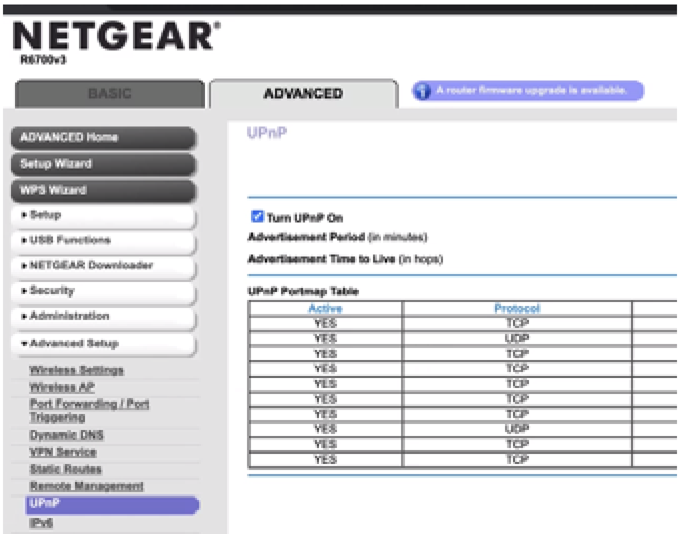
- STAFF AT VICTIM LOCATION WAS NOT IN THE OFFICE UNTIL JANUARY. BY THE TIME THE RANSOMWARE WAS DETECTED, MULTIPLE ITERATIONS OF THE RANSOMWARE HAD EXECUTED.

- WE REMEDIATED THE THREAT, AND REPORTED THE FINDINGS TO QNAP; WHICH USED A 3RD PARTY TO TAKEDOWN THE C2 NETWORK.

ACTIONS FROM THE FIELD

Key Findings and recommendations

- ◇ Check existing device configurations regularly. uPNP enabled the breach to occur. No hardcoded keys exist and the key used to generate the initial encrypt key was destroyed during a power event.



UPnP

☑ Turn UPnP On

Advertisement Period (in minutes)

Advertisement Time to Live (in hops)

UPnP Portmap Table

Active	Protocol
YES	TCP
YES	UDP
YES	TCP
YES	TCP
YES	TCP
YES	TCP
YES	TCP
YES	UDP
YES	TCP
YES	TCP

The AV solution in QNAP flagged all encrypted files, and not the ransomware

- ◇ Mcafee did not detect this ransomware. Had the AV been enabled, it would have not mattered since it was a new malware binary that the vendor did not have catalogued.
- ◇ The AV was disabled and had no associated license. All storage devices that contain business documents, videos, pictures, pdfs can and will be ransomed if left unprotected.

EFFECTS FROM OF OUR INVOLVEMENT ON DAY 1 AND LIMITATIONS OF ACTIONS

- ◇ **CompSec Direct helped the victim isolate the threat, and began recovery efforts.**
- ◇ The ransomware did not have encrypt very large files. Ransomed files will exist in other places, such as other devices, emails.

RECOMMENDED BACKUP/REMEDIATE AND HARDEN STRATEGY

TIME-LINE OF OUR INVOLVEMENT: DAY 02

- ◇ We pushed the threat actor access off the network. Provided documentation demonstrating electrical damage.
- ◇ We consoled the victim that seemed like all is lost. We ensure that our customers understand that events like this is not the end of the business; nor them.

DAY 2 PROPOSAL DELIVERY

CREATION OF SOLUTION

IMPROVED NAS STORAGE

plan to include redundancy locally using TrueNAS and remotely on AWS S3. A custom device buildout was created for high-speed local transfers.

LONG TERM COLD STORAGE

using AWS S3 Glacier for data that is not accessed, but needs to exist. This reduces costs significantly over many years. A thumb drive in owners residence is better than no other backups.

ARCHIVING STRATEGY

using data labelling, we classify information to reduce hunting for files across file systems. This allows company to reduce overall data storage, and costs while creating user access restrictions within work roles.

> “ It is very common to see organizations share an excessive amount of folders, and shared drives across both small and enterprise businesses. This creates opportunities for ransomware where most users can overwrite or delete existing files. Our Insider Advantage program helps organizations determine their level of risk from employees, and in this case, ransomware as well”
> **IT providers make mistakes; some lack security awareness.**

EXIT FROM ENGAGEMENT

TIMELINE OF INVOLVEMENT: DAY 2 END OF DAY

We recommended that the organization should invest in preventative technologies. This included a Kleared4 Edge node with Firewall option. This would ultimately prevent similar attacks from occurring. The configuration also included automated log analysis within our SOC.

DAY 3 –PREVENTION OPTIONS

HARDFACTS ARE ALWAYS TOUGH TO BREAK

Ransomware evolved from past mistakes

Recovery was not possible at the time of this engagement. We recommended cold storage of the device until a tool is produced. Go function mapping was accomplished with a 3rd party tool.

STRATEGIC RECOMMENDATIONS

INVEST IN PROVEN PREVENTATIVE TECHNOLOGIES

Vendor Hype is countered with proven results

Vendor next gen, AI, ML claims rampant, yet these are old problems. An ipfilter could have stopped this.

Develop & test DR process

Backup/recovery scenarios to test effectiveness of disaster recovery strategy, before an incident.

CompSec Direct briefed the victim on efforts with vendor and CISA

We provided a comprehensive report after validating that our preventative measures functioned. A follow up brief was performed after the C2 was reported to CISA.

Have existing incident response on retainer

Incidents beyond ransomware are occurring everyday. Companies must have a pool of vendors to call when problems arise. Some companies that have zero dollar retainers will bill you at a much higher rate than smaller, more agile companies. Negotiating incident response services during a breach places tremendous stress of staff and stakeholders. This also places the victim company at a disadvantage where sound decision making is clouded by lack of business continuity.

ECHORAIX

CLOSING THOUGHTS

Conclusions

Opportunity for improvements

1. Refining triage scripts and lessons learned
2. Preventative hardening is key
3. Power off all equipment during extended breaks
4. Test external perimeter after hardware changes

- ☑ echoraix recovery keys for late 2021 binaries are not yet available. A master key could release in the future.
- ☑ Our Kleared4 range has the samples, and are used during our Using Containers to Analyze Malware at Scale class.
- ☑ Both students and experts have looked at traces, memdumps, and pcaps with no hardcoded keys found.
- ☑ Incident response and malware analysis are expensive; focus on what your customer needs if you are an MSP.
- ☑ Hunting and repoting on threat actors (TA) may bring unwanted attention to yourself and your employer; hire experts to reduce fallback on TA research.

WE ENCOURAGE YOU TO CONTACT US FOR LONG-TERM STRATEGIC SOLUTIONS AND PRICING OPTIONS

www.compsecdirect.com
infopr@compsecdirect.com

☎ (443) 345-0503

151 Suite 200, San Juan,
PR 00901

Recommendations

Hackers will find ways to breach your infrastructure regardless of business trade. Invest in defenses you can manage with a small staff.

Ransomware payments by others resulted in failed data recovery. Seek companies that can reduce your liability and exposure during similar incidents.

Small office and home office IT equipment has security a tradeoff…“Lo barato sale caro.”

CompSecDirect is a C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) security firm that specializes in Information / Cyber Security. We are a service-disabled veteran owned company with an incredible talent pool comprised of former DoD network operators within different sectors of the federal government. The majority of our employees have undergone intensive background-checks by Federal Agencies within the last two years, making them trusted individuals within the intelligence community and private sector. Trusted Individuals is one of our main differentiators to other organizations.

Publishers Note: The contents of this case study are not authorized for use in the press, is not suitable for referencing nor serves as testimonial evidence for use in legal preceding’s without the expressed notification, consent and approval from Comp Sec Direct LLC.