Journal of Cyber Forensics and Advanced Threat Investigations

CFATI

Volume 1(1-3), 47-52. https://doi.org/10.46386/ijcfati.v1i1-3.19

Data Security for the SME

John William Walker[1]

Abstract

Whilst much discussion takes place within the Cyber Security Industry, and at annual events, such as yearly Infosecurity show held in London, with emphasis on the corporate world of security, very little attention given to the often forgotten (ignored) smaller enterprise and millions (billions) of end users who face the very same cyber-threats on an everyday basis. However, this imposition is further compounded by the fact that generally, most of those within the SME sector, and ordinary end-user individuals can be deficient when it comes to cyber-defences, with a much lower level of cyber security savvy skills, which by inference exposes a soft-belly of low hanging fruit, manifesting in a significant surface of attack open to abuse by cyber criminals. In the current age of insecurity, such exposures are particularly noteworthy as threats posed by the potential of encountering a Ransomware attack may be concluded to be significant. This paper looks to outline the threats of the current age of 2020 posed by Ransomware and focuses on how the overlooked SME and Individuals may secure their most precious data object, and their business with affordable, simplistic tools and practices.

Notes for Research

- A Research was conducted into the ongoing lack of attention given to securing the masses of end-user individuals, and of course the enormous global footprint of companies who employ less than 250 people – AKA the Small Medium Enterprise (SME).
- The Research then went on to consider the most common and dangerous of popular criminal attack tools in the form of Ransomware, and investigated the popularity, impact, and growth of such aggressive cyber tools. However, here focus was given to the *larger* groups of *small* end-user individuals and the SME Sector who are a risk.
- Finally, based on serving up a pragmatic, workable and affordable security solution to meet the demands of security for the data, market research and testing was conducted to discover a practical solution which are presented in this paper.

Keywords

cybersecurity, DFIR, ransomware, malware attack, infostealer, malware campaign.

Submitted: 07/09/2020 — **Accepted: 25/**12/2020 — **Published: 15**/02/2021

Corresponding author [1] Address: School of Science & Technology,Nottingham Trent University, 50 Shakespeare St, Nottingham NG1 4FQ

1. Introduction

In the current 2020 era of *cyber insecurity* and the associated everyday logical dangers impacting both global organisations and individuals alike, with the resulting effect on the economy being significant in financial loss realised by an extraordinary amount in the form trillions of dollars. We also see, what has become an almost everyday encounter of the security breach or leak which manifests in exposure of sensitive business and and end-user customer data.

2. The Threats

The logical risks are now proving very difficult to keep up with, and pose a significant overhead on even those organisations who have technological resources. However, even more worrying is the multiple millions (billions) of individuals who are using the Internet to service their every day life needs – individuals who may be asserted to have very little, or no understanding of the actual threat, and even more of concern, how to mitigate and/or recover from such adverse conditions. Risks vary from and morph in many forms which implicate the end target systems, with one very current example being that of a Ransomware attacks which are crafted with the malicious intention of compromising a device to lockout the authorised user from their own data objects; *or*, even locking out the entire system from user access. One example of such a Ransomware application was uncovered

in 2020, titled Ransom EXX which is known to have infected the headquarters of the Japanese company Konica Minolta with devastating effect – Ransom EXX is so new, as of today 8 August 2020 very little is known about this malware application – See **Fig 1** below.

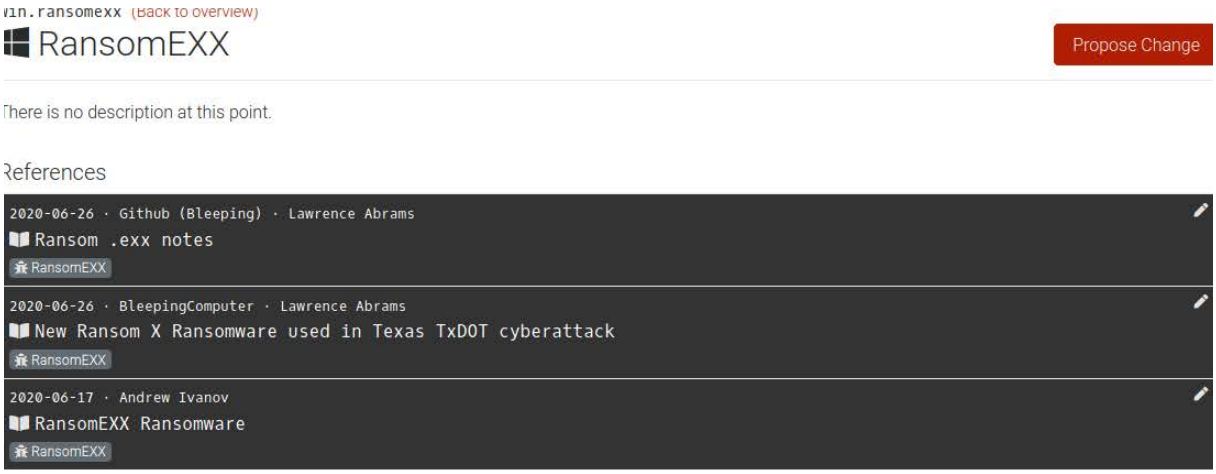

Figure 1. Ransom EXX Knowledge Base

The threat posed by the ever-invasive associated Advanced Evasion Techniques (AET) of Ransomware attacks arrive in a profile which is developed to technically encourage the recipient end users by a precursor Phishing communication into clicking the presented malicious link(s) to invoke the activity of infecting the system – with the criminal usually offering to re-enabled access based upon a nominal payment of around $350 in the form of a ransom fee. **Fig 2** demonstrates the increased spread of popular Ransomware agents from January 2017, up to May 2019.

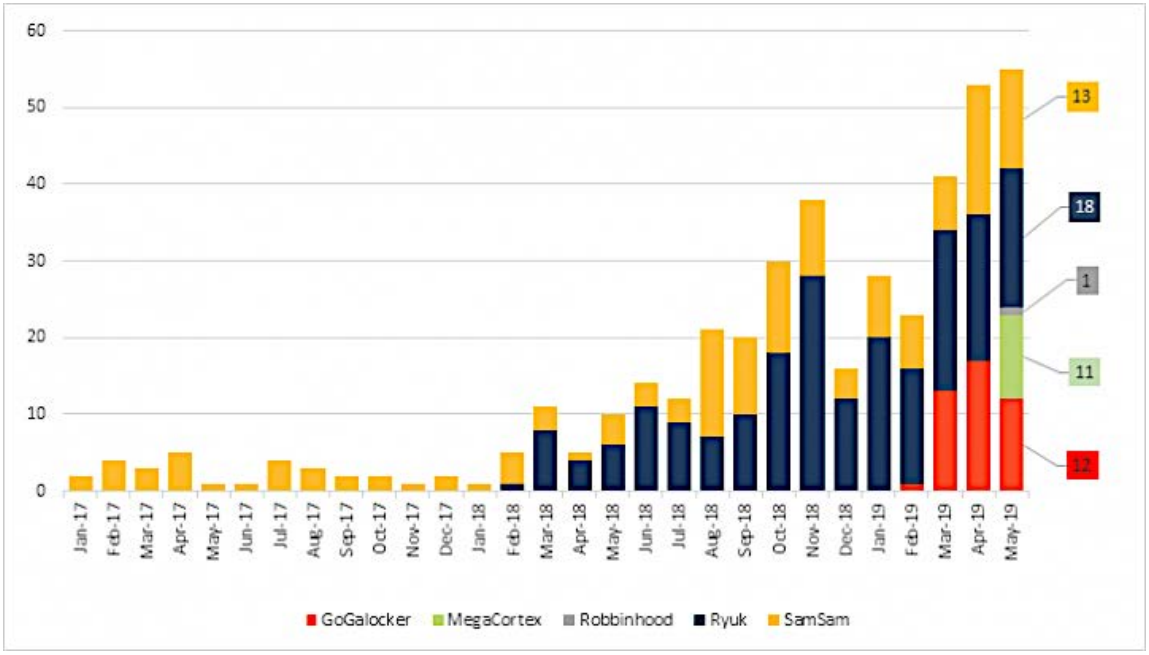

Figure 2. Ransomware Growth 2017 – 2019 (Symantec-Security-Response-Team, 2019)

The process used to deliver a Ransomware agent is multi-threaded, involving the creation of the mal-application, the enterprise infiltration to reach the end-user screen, and then the careless mouse-click to invoke the delivery of additional objects

from the Internet, leading to the seek-encrypt-lock process of any systems within the logical patch of the malware agent – See **Fig 3** below:

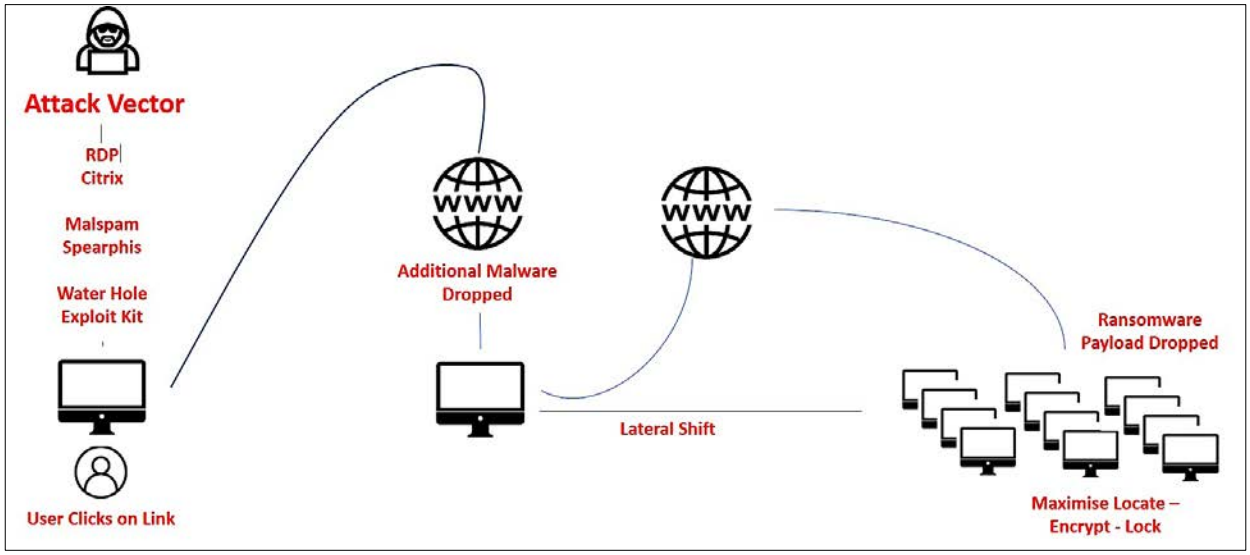

Figure 3. Example of Ransomware Enterprise Infiltration

3. The Legal Position of Paying a Ransom

As a side conversation, in research conducted into the holders of Crypto-Currency (the untraceable currency of the Ransomware Criminal Fraternity) it can be discovered that many large institutions have been known to keep a handy cryptowallet as a backup resource, just in case they get unlucky and fall victim to a successful incursion – and here we are aware from a number of unpublicised occurrences, big name companies have actually paid over said ransoms in hope that their data will be unlocked and restored. However, it is here where the grey line of legality may bring doubt, as when such a payments are made, this not only potentially breaches any active AML (Anti Money Laundering) Policies, but also can manifest in a potential criminal act insofar the paying criminal organisation may be directing funds into a criminal and potentially terrorist based organisation. This in turn in a number of instances can also breach CTF (Countering Terrorist Funding) – see reference (Force, 2008) Financial Action Taskforce 'Fighting Terrorist Financing', which infers that to pay such demands goes on to provision funds to support other related criminal activities, ranging from the production of counterfeit goods through to people trafficking.

4. Big Picture First Hand Case Studies

To bring the subject of Ransomware into alignment with a real-world of hands-on operational encounters, we may focus on a case study which relates to the unnecessary impact of a Ransomware attack on a well-known UK brand located within the hospitality sector. The first indications of the presence of a Ransomware agent being resident on a server within the organisations on-site farm was detected by a third-party SOC (Security Operations Centre) located in the US who informed the client on each monthly service call that they were hosting what looked to be a viral agent. However, given that this particular business was running without a *senior*, *knowledgable* security lead, the incumbent *junior* interim security manager decided that, as this particular agent was passive and not causing any issues, it would be dealt with at some future juncture as a matter of routine maintenance when that particular server would be subject to update, and thus in the meantime the threat vector was allowed to remain passively active and resident on that particular machine. The unfortunate impact was realised when a wandering mouse-click of an internal user found the said Ransomware agent, and with one click the adverse payload was invoked – a process which locked down 7 production servers, and one front of house system serving as a payment kiosk for hotel guest, hosting multiples of PCI-DSS transactions. However, this particular Ransomware agent had a number of other adverse facets, and it was soon discovered from a packet sniff that this Ransomware agent was also calling home and sending packets of data out to an offshore IP address – possibly credit card transactional data. As more in depth analysis was conducted it soon became very clear that this particular agent was smart, as it also took steps to *locate* and *disable* any on-system anti-malware protective defence on the booking workstation! The overall impact was lost revenue, 6 days of a clean up operation, and the small matter

of reporting the breach under the PCI-DSS *mandated* processes, which was action *never* taken!

There are of course many other examples of successful Ransomware attacks which have caused significant disruption beyond that of the technological impact. One example of which is the case of the Lincolnshire County Council way back in 2016 who were under the management of a Serco outsourcing contract, reported in the press to have received a ransom demand of £1m. In this case, so bad was the disruption caused to the authorities data, the councils sub-divisions were so adversely impacted that they could not process accounts, pay invoices or service their schools with supplies. Needless to say, whilst the incident was played down, it did cause the authority to claw back funds from Serco as a fine for their blundering and mismanagement.

In the aforementioned case studies, these organisations were large, with technical resources to hand to recover the data from the last backups where possible, and to interact with the clean-up operation, and of course to carry out post attack measures to secure the enterprise with new configurations and defensive application upgrades. It is here however where one may conclude that those who's sensitive and business data assets are at the greatest risk of exposure are within the communities of the multiples of members of the everyday end-user public, and of course the business domains of the SME, who according to research carried out by RICOH (Gammelgard, 2020) concluded that there are vast opportunities for the criminals, with 58% of UK based SME's paying the ransom. A second report (Sjouwerman, 2020) published by Knowbe4 reported that they had noticed the trend of attacks were occurring at a rate of 1 every minute, again implicating SME's which accounted for 62% of Ransomware attacks. Given that the SME sector can tend not to accommodate adequate resource in the form of a technical cyber-savvy security posture and support capabilities they clearly represent a very low hanging fruit target for the passer by cyber-criminal looking for a soft-belly – which is why, to date multiples of such smaller users targets have suffered the very real consequences of data-lockout, most of which first hand experience has proven, they actually paid over the ransom in order to save their business from extinction due to denied access of their critical operational data.

5. Landscape of Exposure

Looking back over the last decade in which Ransomware attacks have become a crafted money spinner for organised cyber-criminals, the real vulnerable exposure points have been twofold:

- Lack of up-to-date backups
- Easy access to data assets

Taking the first vulnerability on its merits, if organisations have maintained a life-cycle of current backup strategies, in the recovery posture they may then have an opportunity to revert back to the last current data image and restore it – following up with a complete restoration of the corrupted systems. But as has been exemplified in so many Ransomware attacks, particularly in the cases of individuals and the SME Sector, such backups are not always available, leaving only one option of response to the loss of data - that being paying the ransom demands in hope the compromised data may be unlocked.

The second option is to take the *proactive* steps around data availability, and here it is in the *proactive mode* where the end user and SME may take action, not only in the form of backing up, but also by denying the opportunity of data corruption and compromise by securing the valuable data assets in what may be considered an *untouchable* state. With larger businesses, they do have many options in the form of enabled areas of protected storage such as SAN (Storage Attached Network) and NAS (Network Attacked Storage), but for the multiples of end users, and the SME Sector, again this may be something that is technically out of reach, technically challenging and cost prohibitive. So, for the individual, or small business users alike, there is a very necessary and urgent need to serve a proactive defence to secure their valued data assets.

6. Logical Chain Security

Whilst we may assert that the larger commercial, and cross sector organisations and institutions are in a position to strengthen their approach to mitigating the threat, and to maximise their defensive posture, there is need to urgently consider how the most exposed and vulnerable surfaces of potential attack are accommodated with a sensible, affordable and realistic cyber defence to secure their digital assets (data/information). So here we look to enhancing the security profile of the overlooked billions of ordinary users of the Internet, as well as those resident within the SME sector to mitigate and reduce the opportunities Ransomware agents success of lockdown.

But it is not only Ransomware which may implicate valuable end-user data objects. In August 2020 the Microsoft Security Intelligence Team reported on the Anubis Malware Agent which looks to seek out financial information assets, as well as those valuable cryptocurrency wallets which are open to access – a further reason why such valuable data assets should be stored off-line. See Fig 4 below relating to the Anubis (Hashim, 2020) Malware Agent.

Figure 4. Anubis Cryptocurrency Stealing Malware Agent

Given that the target is the actually the data, if such valuable assets are secured in a logical/physical location, then it must follow that if the users are unlucky enough to click on a link which does invoke a Ransomware process, granted it may be that the local system files, and even the local computer may become unavailable. However, as the malicious agent cannot follow an active, available logical path to the crown jewels data objects, then they are completely safe. This simple, yet effective solution may be affordably facilitated with a secured drive with pin-access ACL (Access Control List) such as a diskAshur DT (iStorage-DT) (Desk Top) unit for the SME, and in the case of the everyday user a diskAshur Pro (IStorage-Pro) will serve an effective solution to protect the data at rest. Thus enable speedy recovery time and effort post attack – even if the drives are connected, but not authenticated the Ransomware can't gain access to the contents. At **Fig 5** is an example of the type of drives which may be used to secure data under attack from a Ransomware agent:

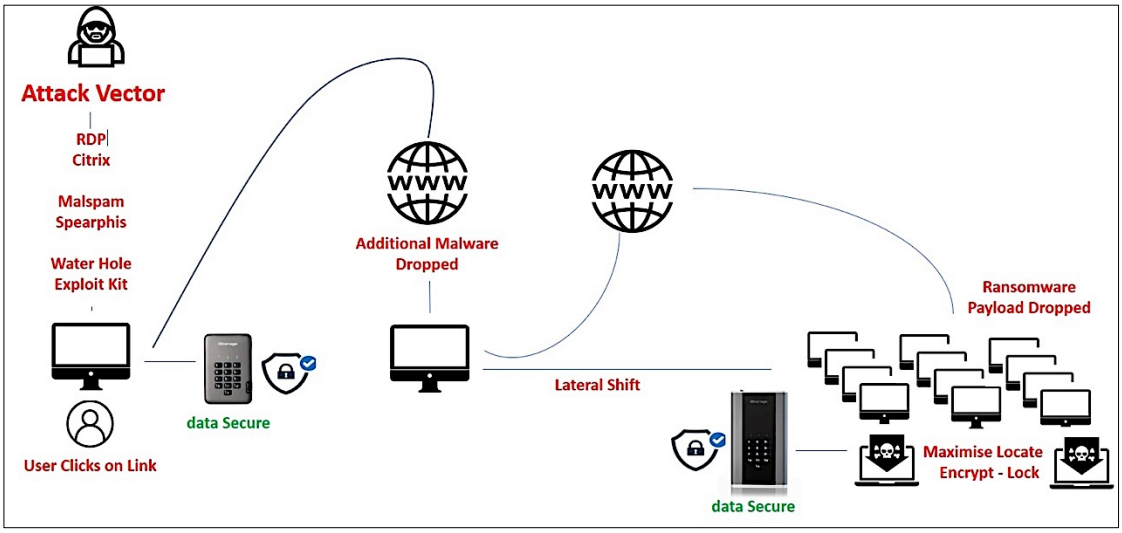

Figure 5. Secured Data with ACL Protected Encrypted Drives

The final state of recovery would now be simply to reinstall the O/S which is not an arduous process for any user with moderate skills – failing that a visit to a PC Store will accommodate the recovery.

7. Conclusion

On the premise that cyber-insecurity will not go away anytime soon, against the backdrop of regular breaches of security which

leak end-user data into the hands of criminals, we must consider the individual and the SME to be a target on mass. Add to this the fact that such small users may be devoid of any expertise, then one may conclude they is an on-mass set of targets that are subject to exploitation every single day. Such simple solutions as suggested in this paper, may be considered by those with the technological security prowess to be simplistic. However, for those individuals and SME's who use the Internet to conduct their everyday life, and business practices, such simple solutions as introduced may be considered a business life saver. If we are to start to put a dent in cyber-crime, we must place focus on the masses of end users and start to think small to mitigate the mass exposure of the vulnerable, forgotten end-user public.

.

Declaration of Conflicting Interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) declared no financial support for the research, authorship, and/or publication of this article. Or please insert other relevant information here.

Acknowledgments

To the creators of iStorage.

References

Force, F. A. T. (2008). Countering Terrorist Funding. Retrieved from https://www.fatf-gafi.org/media/fatf/content/images/TF-operational-reports-brochure.pdf

Gammelgard, M. (2020). Ransomware attacks are successfully targeting small to medium-sized businesses – how do you protect your data? Retrieved from https://insights.ricoh.co.uk/simplifying-technology/ransomware-attacks-are-successfully-targeting-small-to-medium-sized-businesses-how-do-you-protect-your-data

Hashim, A. (2020). Microsoft Warns Of Another 'Anubis' Malware Targeting Windows. Retrieved from https://latesthackingnews.com/2020/09/02/microsoft-warns-of-another-anubis-malware-targeting-windows/

iStorage-DT. diskAshur DT. Retrieved from https://istorage-uk.com/product/diskashur-dt2/

IStorage-Pro. diskAsure Pro. Retrieved from https://istorage-uk.com/product/diskashur-pro2/

Sjouwerman, S. (2020). Ransomware Incidents Increase 131 Percent with the SMB Being the Primary Target. Retrieved from https://blog.knowbe4.com/ransomware-incidents-increase-131-percent-with-the-smb-being-the-primary-target

Symantec-Security-Response-Team. (2019). Targeted Ransomware: Proliferating Menace Threatens Organizations. Retrieved from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/targeted-ransomware-threat