The Evolving Threat of Ransomware: From Extortion to Blackmail

Dr. Lena Y. Connolly, Assistant Professor, College of Technological Innovations, Zayed University, alena.connolly@zu.ac.ae (corresponding author)

Dr. Michael Lang, Senior Lecturer, Business Information Systems Group, National University of Ireland Galway

Paul Taylor, Force Relationship Manager, National Management Centre, UK

Phillip J. Corner, Industrial Cyber Resilience Engineer, Cougar Automation Limited, UK

***Abstract*—Ransomware is continually evolving. The most recent tactic is to combine crypto-ransomware with data exfiltration, mandate fraud, and other such schemes to steal from victims and attempt to blackmail them. This paper examines the new trend, its underlying motives, and proposes practical recommendations to help organizations defend against this menace.**

***Keywords*—Ransomware, Data exfiltration, Blackmail, GDPR, Incident response**

I. Introduction

In this article, we consider the unrelenting rise of ransomware attacks and put forward some guidance to mitigate this threat. As starkly evidenced by a recent international survey of 5,000 IT managers, the incidence of ransomware attacks is growing exponentially [1]. In the past year, we have witnessed the emergence of attack strategies unlike anything ever previously seen. As organizations have improved their defence mechanisms by deploying effective backup strategies, criminals in turn have adopted methods that increase the potency of their assaults. This new *modus operandi*, which we refer to herein as hybrid cyberattacks, aims to maximise the financial gain by committing more than one crime within a single breach. Instead of just going for a “quick win” of executing ransomware, which only in a relatively small proportion of cases yields a return, cybercriminals instead stealthily infiltrate the organization’s systems, seek to exploit as many opportunities as possible by means of mandate fraud, data exfiltration, or other methods, and then drop ransomware as the final coup.

The amount asked at this point is usually very high because attackers have accumulated comprehensive knowledge about the organization, its data and systems, the consequences the attack will have, and their ability to pay. For example, the University of California San Francisco paid US$1.14 million in bitcoins following data theft and a subsequent ransomware attack. Similarly, the University of Utah paid US$457,000 to prevent a data leak. Such high yields send a signal to cybercriminals that they can profit handsomely from their actions, and they will unscrupulously persist to exploit these opportunities until such time as they cease to be lucrative.

Conquering the threat posed by cybercriminals has never been more important. The burning question is how do we achieve this? Ransomware, data theft, mandate fraud, systems hijacking, and other such crimes are not new, and a myriad of well-established technical and procedural countermeasures to tackle them exist [2]. However, despite all these advances, there is no sign of things abating. Cybercriminals continue to prosper, now worryingly directing their attacks towards public services and critical infrastructure [3].

There are very few empirical studies of ransomware attacks in the literature (e.g. [4,5,6,7]), not least because victims generally do not wish to publicise the fact they were breached. Even if it becomes known that they were, they do not wish to speak about it. Indeed, there are a number of cases where organizations denied that they were attacked, even though corporate data was leaked on the Dark Web. However, this tactic can sometimes be a ruse [8].

What must we do to mitigate the threat of a hybrid attack? This is the question that we explore in this paper, using qualitative data drawn from interviews with cybercrime police detectives, industry experts and ransomware victims from the UK and Ireland. To preserve anonymity, aliases are used to refer to individuals and organizations in the following sections.

We begin by briefly tracing the history of ransomware and explaining how the most recent variant differs from what went before. We then set forth a number of practical

This work was supported by the Engineering and Physical Sciences Research Council and is part of the EMPHASIS (EconoMical, PsycHologicAl and Societal Impact of RanSomware) project [EP/P011721/1]

L. Y. Connolly is with Zayed University, Abu Dhabi, UAE (e-mail: alena.connolly@zu.ac.ae).

M. Lang is with the National University of Ireland Galway (e-mail: michael.lang@nuigalway.ie).

P. Taylor is Force Relationship Manager at the National Management Centre, Manchester, England.

P. Corner is a Senior Security Consultant at Cougar Automation

recommendations to counter this evolving scourge.

II. Ransomware evolution

Connolly and Wall [2] trace the history of ransomware over the past three decades, identifying a number of evolutionary milestones marking the emergence of what they call Generation I, II and III. The first of these came in 1989 when a form of crypto-ransomware was distributed on floppy disks amongst participants at the World Health Organization AIDS Conference. This variant employed weak symmetric cryptography to scramble victims' files and was incapable of propagating on networks beyond the infected device.

The second generation (e.g. CryptoLocker) took off about 2013 and utilised virtually unbreakable asymmetric cryptography. Cybercriminals adopted an opportunistic "spray-and-pray" approach and made very sizeable profits by extorting relatively small amounts from a large pool of victims. Generation II ransomware can spread to devices that are physically or logically connected to the infected machine. Ultimately, Generation II aimed to infect shares on a server, providing that the user has a 'write' access to the server.

The next landmark came about 2016 with the emergence of Generation III crypto-ransomware (e.g. Samas), which was driven by hackers' growing appetite for larger bounties. These variants have advanced propagation capabilities and can infect entire servers and even networks. Generation III ransomware also changed tactics, moving away from the mass infection approach towards targeting specific organizations, with the aim of extorting very high amounts of money from each victim. This "big game hunting" strategy involves the cybercriminal conducting substantial pre-attack reconnaissance, and quite often the attack vector is spear or whale phishing. As one of our police interviewees remarked:

"Before, it was more of a shotgun approach. If they got a payment, great. If they didn't, no problem because the next person might pay. But then everything became a bit more targeted, a bit more purposeful." [Detective Sergeant, CyberTL]

The latest evolution of ransomware, referred to as Generation IV in this paper, is very audacious. In addition to scrambling files and demanding a ransom in exchange for a decryption key, attackers also conduct other crimes, including mandate fraud, system hijacking and data exfiltration. Stealing data is becoming a particularly popular trend. If criminals manage to transfer valuable information to an attacker-controlled location, this gives them an opportunity to blackmail victims. According to a recent report, 30% of ransomware attacks in the second quarter of 2020 threatened to release exfiltrated data, and 22% of attacks actually did so, which was a very substantial rise from the first quarter [9].

The reason that attackers have added this extra sting is because they were starting to find it difficult to extort payment using ransomware alone, as many organizations had put effective backup strategies and other defence mechanisms in place to mitigate the threat [8]. A detective shared her recent experience with us:

"Something that I have observed of late is the increasing success of companies in recovering from ransomware infections without having to actually negotiate with the criminals. Consequently, attack tactics have changed. Hackers now make every available opportunity profitable once they gain access to a victim network. Before executing ransomware, they will commit mandate fraud, or extract data, or they may use systems for criminal activities. This is not something we have previously seen; it is a new threat from our perspective, and – worryingly – we have seen much more of it recently." [Detective Sergeant, CyberTL]

A summary of the differentiating characteristics of the evolving generations of ransomware is presented in Table 1.

III. The blackmail element

Early generations of ransomware focused on extortion or a threat to wipe data by destroying a decryption key. Generation IV ransomware introduced a blackmail dimension, intimidating victims to expose stolen data and preying on their various fears of (1) incrimination (e.g. exposure to data protection authorities), (2) reputational damage/lost revenue (e.g. exposure of sensitive data which could cause loss of customers), (3) exposure of intellectual property, and (4) humiliation (e.g. exposing embarrassing information about customers or a particular employee in an executive role). These attacks are highly targeted in the sense that thieves search for specific data on victims' networks and only take what is valuable.

A. *Fear of incrimination*

With the emergence of the General Data Protection Regulation (GDPR), which carries harsh penalties for non-compliance, attackers attempt to blackmail victims into submission. As one of our police contacts explained:

"We've started to see this new method of operating where [in addition to ransomware], criminals take victims' data, copy and put it somewhere else. They then threaten to publish data if victims refuse to pay. Criminals also blackmail victims with the GDPR requirements. They explicitly explain the problems that the organization will be facing if the data breach becomes known to the data protection authorities." [Detective Constable, CyberTL]

Penalties for breaking GDPR requirements can be very severe. For example, the UK's Information Commissioner Office (ICO) fined British Airways £20 million for failing to protect personal data of more than 400,000 of its customers [10]. According to the GDPR, organizations that collect personal data of European Union citizens and residents must follow a set of standards to safeguard the processing and movement of this data. One of our interviewees, however, disagrees with the penalty structure enforced by the GDPR and suggests a different approach:

"Too many cyber incidents are kept quiet because of fear of incrimination. Organizations are afraid of prosecution by information commissioners. So, the ICO have got to rethink and have some mechanism in place to encourage companies to report. Like a parking ticket – if you pay the parking ticket within 14 days, it is only £20 instead of £60. So maybe with the GDPR, they should say, 'If you tell us on Day 1 that it happened, we will be lenient towards you. But if you tell us two weeks later, a month later, or longer, then you are going to get the full force of the law'. There has to be some way to take into account the honesty of the organization. Otherwise you are creating another problem by fining them such a huge amount" [Security Manager, GovSecJ]

In order to intensify the blackmail attempt, criminals share details of location of the stolen data and even allow victims to access it. A detective shared his observation with us:

"Attackers often inform victims that their data is being held at a certain address and provide a username and password as 'proof of life'. This has happened in a number of cases in exactly the same way, where victims were blackmailed with GDPR." [Detective Sergeant, CyberTL]

B. *Fear of reputational damage and lost revenue*

An alternative pathway that attackers take is threatening the victim to publish confidential customer information on the Dark Web. This tactic preys on victims' fear of reputational damage, which consequently can lead to the loss of customers and revenue. Attackers are acutely aware of the potential costs businesses can encounter if customers learn about an incident, especially if they are directly affected. Police officers shared with us a case where a victim ("FinOrg") refused to pay a ransom although customer confidential information was copied and transferred to the attackers' location. The victim received a warning from cybercriminals that all the data they stole would be sold on the Dark Web unless they paid. Indeed, such action can potentially lead to secondary crimes (e.g. financial fraud, identify theft) that can have devastating implications for customers, but most importantly for the business is that such consequences could destroy customer trust. Although FinOrg was tempted to pay, they decided not to. They felt that the risk of becoming a victim of indefinite blackmail (i.e. there is no guarantee that attackers will delete data after the payment) was too high. FinOrg made a very difficult decision of contacting thousands of their customers to inform them about the breach.

Although ransomware attacks can be expensive for organizations to remediate, the consequences go far beyond network recovery expenses. Victims are often faced with the loss of business through reputational damage that can take years to repair. For instance, Cognizant Technology Solutions experienced a ransomware attack in April 2020 and reported a rapid revenue decline following the incident [11]. As one industry expert put it [12]:

"Companies are waking up to the reality that ransomware attacks can be very serious and costly. Even when cyber criminals demand a paltry sum, the attack can end up costing hundreds of thousands or even millions due to business interruption and reputational impact."

This is why organizations sometimes choose to pay and restore business operations as soon as possible. As another leading professional elucidated [13]:

"This is a fundamental consumer value proposition. If [a victim organization] were to allow extended downtime, customers would switch off and not trust the organization. If your customers cannot access your product, you'll be willing to pay a high ransom."

C. *Fear of intellectual property exposure or loss*

Attackers also tend to prey on the intellectual property (IP) of victim organizations. Recently, several higher education institutions confirmed ransomware attacks, including the University of California San Francisco (UCSF), University of Stanford and University of California Berkeley. The loss of research outputs can affect a university's IP and revenue stream. In the extreme, it can cause them to drop in international league tables, affecting the number and caliber of academic staff and students. UCSF issued the following statement providing justification for payment [14]:

"The data that was encrypted is important to some of the academic work we pursue as a university serving the public good. We therefore made the difficult decision to pay some portion of the ransom, approximately $1.14 million, to the individuals behind the malware attack in exchange for a tool to unlock the encrypted data and the return of the data they obtained."

Several other examples of data leaks from private companies have been recently reported by the media. Although hackers provided evidence of these data breaches by posting images of stolen data, organizations are often reluctant to confirm incidents. Such reaction does not come as a surprise since an organization's future may be at risk should competitors learn about the theft. Being aware of this, attackers threaten victims to sell IP to their competitors unless the payment is made [15]:

"REvil has created a dedicated auction site for others to bid on stolen data. The prospect of their data being auctioned and sold to competitors is likely to concern companies more than the prospect of simply being posted on an obscure Tor site."

D. *Fear of embarrassment*

Cybercrimes where offenders threaten to reveal information that will cause embarrassment to a victim are not new (e.g. blackmail on social networking platforms). Stealing embarrassing content, however, is a novel approach in the Generation IV ransomware crusade. A well known cosmetic surgery hospital in the UK was held to ransom in this way at the end of 2020. As one anxious customer expressed in a media interview [16]:

"I received an email informing me of a data security incident but no detail as to what has been hacked ... I am obviously concerned as the last thing I want is 'before photos' being splattered around in the public domain. I have tried to keep my surgery private and not even some of my friends and colleagues know about it, so the data breach is concerning me".

If hackers discover sensitive material of a humiliating or awkward nature, they will leverage it to its maximum potential to demand a higher ransom. If, however, the victim declines to pay, hackers will not hesitate to publish embarrassing information. This was the case with Toledo Public Schools (TPS), Ohio in October 2020, where attackers accessed highly confidential information, including disciplinary and disability reports, and published it when TPS refused payment. Ransomware attacks that phish for embarrassing information considerably widen the net of victims, making these data breaches particularly harmful and upsetting.

IV. Practical Recommendations

In a previous issue of this journal, Kharraz et al [17] posed the question as to whether the challenge of protecting against ransomware raises new intellectual challenges, or is it just a case of restating classic ideas. They assert that although much of the defence strategy is the same as would be used to fend off and recover from any other type of cyberattack, there are a number of distinctive considerations that are worthy of further research. Upon examination of the cases described by interviewees, we noticed a number of common weaknesses and shortcomings that enabled these recent hybrid attacks. Based on this analysis, we present the following recommendations.

A. *Preventing data exfiltration*

The blackmail element in Generation IV ransomware is only enabled when criminals manage to exfiltrate data from victims' networks. Worryingly, some victims are not even aware that their data is gone until hackers contact them or it is already leaked:

> *"The victim in a lot of cases does not have full oversight of what has been actually taken from them. My real concern is that once an organization has its network ransomwared, do they have the capability to go back in time and conduct a full audit of whatever activity was happening on the network for the last week, month, or longer. And the answer very often is No" [Detective Sergeant, CyberTL]*

In order to prevent illegal data transfers, organizations are conventionally urged to scan network traffic and monitor unusually high bandwidth utilisation. However, as encryption of the Hypertext Transfer Protocol (HTTP) using Transmission Layer Security (TLS) has become commonplace to help keep sensitive data private on the Internet, ransomware actors have also moved to use it to defeat basic content scanning techniques. In an attempt to address this detection avoidance used by ransomware for data exfiltration, multiple vendors recommend employing TLS inspection. These systems use a public key infrastructure (PKI) certificate authority which is trusted by the organization's computers. This allows a network security appliance to conduct what is essentially an authorized man-in-the-middle monitoring of encrypted traffic. This technology, however, must balance privacy laws against the performance impact of resource-intensive encryption and scanning operations. Solutions often employ vendor- and customer-defined trust lists and fast-path rules for trusted business applications and websites.

Approaches to data theft detection and prevention vary depending on the location of data. Attackers have modified their methods to avoid detection by using business cloud platforms for ransomware downloads and data exfiltration as these platforms are likely to be trusted by organizations and excluded from scanning. This approach may be informed by attackers' research on potential victims' security solutions from publicly available information. Unusually large data volumes may still arouse suspicion. Attackers hence use the 'low and slow' approach of trickling data transfers which helps to blend in with background activity and avoid appearing in high volume reports.

Organizations that have migrated to cloud native data storage and collaboration tools will have to re-assess their information security strategy and may find their on-premises security technologies cannot protect cloud stored data. These organizations are largely restricted to features made available by their cloud service provider. If an attacker succeeds in obtaining login credentials, they can penetrate a network, move laterally, and conduct internal reconnaissance by eavesdropping and rummaging through cloud files. For example, if a Microsoft Office 365 email account were to be compromised, it could give access to an organization's shared documents. Data exfiltration might be as simple as switching to OneDrive or SharePoint and searching for "Confidential", "Internal Use", "Bank Details", "Password", "Curriculum Vitae", "Contract", "Allegation" or other term likely to retrieve classified documents that could be used as leverage to extort payment. Depending on the roles and privileges assigned to the individual whose account was hacked, this could be very serious. We advise to utilize Multi-Factor Authentication (MFA) to prevent unauthorized access, combined with audit logging of user actions. Some organizations are reluctant to adopt MFA because of employee privacy issues (e.g. using personal telephone numbers for SMS authentication), but against this downside the benefits of greatly enhanced security must be set.

Many cloud providers now support Data Loss Prevention (DLP) to classify and control data sharing and may offer 'always-on encryption' through Information Rights Management (IRM). The IRM controls what legitimate logged-in users can do with data (e.g. no downloading or printing) and prevents all access to stolen files without a valid login. As vendors continue to improve their response to attack techniques, some are now beginning to develop advanced integrated approaches, often described as Extended Detection and Response (XDR). The XDR links network, endpoint and other security technologies in their portfolio in an attempt to collectively address the challenges of root cause detection and subsequently prevent infection, lateral movement, and data exfiltration.

There are also mitigating controls that can be employed to reduce the severity of successful attacks. One such control to protect sensitive data is file-level encryption, where data encryption is proactively applied at a file level, so the data is secure against unauthorized access wherever it is stored. Although this does not prevent data exfiltration, it adds protection that helps to render any exfiltrated data useless to the attacker. Commonly available tools for this are generally designed for individuals and utilise simple passphrase-based symmetric encryption. This approach, however, does not scale effectively for large collaborative enterprise environments without complex methods of passphrases sharing, which are also difficult to secure. Some vendors offer proprietary software designed to transparently implement 'always-on file encryption' that works collaboratively for larger enterprises. These, however, are considered a more advanced control and can impose significant initial technical burdens to achieve a configuration that meets the end users' needs, particularly if data classification is not already in place.

As important as technical solutions are, the heart of the problem is that organizations do not identify their risk exposure. They do not know their data (i.e. lack of classification mechanisms) and, most importantly, are not aware of its location. This is equally applicable to identification and classification of critical systems. The DLP solutions may operate at the network level similar to TLS inspection, or endpoint level via an agent to help organizations classify sensitive data as well as detect and prevent unauthorized transfer of any sensitive file. Some organizations do not employ data access audit logs and hence maybe not be able to identify the scale of data theft without engaging with the attackers. In such cases attackers can claim that they accessed and stole a lot more data than they actually did. Centrally collecting access audit logs from critical assets gives incident responders vital data to investigate should an exfiltration attack be successful. The ability to validate an extortion claim and assess the damage is invaluable [8]. Furthermore, once logging is enabled, organizations can employ more advanced automated analytics like Security Information Event Management (SIEM) solutions. SIEM utilizes machine learning models to detect indicators of compromise with the noise of routine activity in log files.

Ultimately, prevention is better than cure. Focusing solely on detection and failing to adequately address security fundamentals leaves systems open to attack. Organizations must ensure they have undertaken basic hardening and best practice as a foundation on which to deploy more advanced security products from vendors. A number of basic controls can be implemented in existing infrastructure to significantly reduce risk of infection and increase visibility. Crucially, it is impossible for any system to be absolutely secure and no one product or technology offers a 'silver bullet' against ransomware. In practice, the application of multiple complementary controls, known as defence-in-depth, is vital to reduce the threat of ransomware, especially as techniques, tactics, and procedures of threat actors continue to rapidly evolve with new generations of ransomware.

B. *GDPR – Be Vigilant and Fear Not*

An organization that fails to comply with the stringent requirements of GDPR is liable to be fined up to 4% of its global turnover, depending on the severity of the offence. Although not as punitive, provisions for fines have recently also been introduced or proposed in other jurisdictions such as Switzerland's Data Protection Act 2020, Brazil's LGPD 2020, and India's Personal Data Protection Bill 2019.

Unscrupulous attackers attempt to use the prospect of fines to their advantage by threatening to expose failings to the relevant enforcement agency unless a blackmail demand is met. Although changing the fine structure could be a potentially good solution and is worthy of further exploration, the best defence as of now against this ploy is for organizations to regard GDPR not as a burden but rather as a 'gold standard' that serves to improve cybersecurity. It obligates data controllers to systematically catalogue the location and scope of all personal information, methodically analyse infrastructure, define policies and procedures for data storage and transfer, and put strong governance in place. Being GDPR-compliant not only safeguards citizens' rights but also protects organizations by making them more resilient in the wake of a ransomware attack and cutting off an avenue for blackmail.

If an organization can demonstrate that it adhered to the rules, the risk of monetary penalties or civil action is dissipated. Under GDPR, it is not a requirement to issue notification of a ransomware attack unless personal data that presents a risk to the affected individuals is breached. However, in order to make this determination, organizations need a rigorous risk assessment process and robust procedures for detecting, investigating and reporting breaches. It is therefore seen that GDPR is not just a sword but also a shield; rather than being fearful, organizations should embrace it.

C. *Knowing how to respond when calamity strikes*

One of the first steps that employees need to take if they detect a suspicious activity is to report it without delay. Although many organizations directly employ or hire the services of staff to provide around-the-clock physical perimeter security, when it comes to IT security, very few organizations have 24/7 guards looking out for suspicious behavior. Consistent with the observations of previous reports [18], our interviews revealed a pattern of attacks occurring at night, weekends or holiday periods. Attackers deliberately choose this timing because normally there are fewer IT staff on duty, if any at all, to monitor alerts or to take notice of network performance issues. As one of the police officers noted:

"The weekend is a good time to target any company because everybody leaves work at 4 o'clock on a Friday and do not come back until Monday. It is good because organizations have minimal staff in." [Detective Constable, CyberBR]

Another expert interviewee explained a typical scenario as follows:

"You're the manager of a small firm and you've had a fairly rough week. Come Friday evening, you're winding down at home, enjoying a pizza and a glass of wine when unexpectedly the phone rings ... 'Hey, boss, it looks like we've just been hit' ... and then panic strikes and you start thinking about how to salvage your most valuable assets. It's like the house is on fire and you have to quickly grab the things that matter the most to you." [CEO, FortNet]

We feel that all organizations should consider out-of-hours IT security monitoring and support. If an employee's single sign-on password is compromised while working at home over a weekend, it cannot wait two days to be rectified. Cybersecurity-as-a-Service (CSaaS) is increasingly being adopted as an option by organizations who do not have the capability to provide continuous in-house cover.

Most importantly, employees need to know when to contact IT. The very first response steps will define the outcome of the incident. One of the affected organizations ("LawEnfJU") shared that while their employee detected a suspicious activity (i.e. files on a shared drive were encrypted and therefore were inaccessible), they shut down their machine and logged into another. This step was repeated with several machines until the employee finally realized that they needed to contact IT.

Fire drills are required by law in several countries and employees know precisely what to do when alarms sound. In contrast, very few organizations run regular IT security drills, so employees typically don't know how to respond when suddenly faced with a cyberattack as was the case with LawEnfjU. Lack of awareness and preparedness was a common theme across the cases recounted to us by police officers.

It is not sufficient just to have an incident response plan and links to training videos that employees are told to watch. Organizations should simulate phishing and ransomware attacks on a periodic basis so that employees know how to recognize potential risks and proact or react accordingly. A Security Manager from a victim organization shared his opinion of what ought to be done to prevent further attacks:

"I have a military background, and this is what we do in the army – we train people how to act in case of an attack. The same should be done in organizations to protect against cyberattacks. It is called a tabletop exercise. You simulate attacks and teach people how to react if a cyberattack happens." [Security Manager, GovSecJ].

Another interviewee emphasised the importance of having a very clear incident response strategy:

"Ransomware attacks are fantastically interesting. I like getting into the details of the poor folks who got caught to see what went wrong. And what emerges is how really important it is to have a plan in place that covers the basics, and to practice that all the time. If you're constantly practising the basics, they become habits and will come naturally, just like great sports teams. But if there is no plan and the enemy strikes, you won't have time to think about the stuff that you didn't expect. For example, if you get hit by ransomware, who's your chief negotiator, have you considered that? You need to have practised your negotiation plan to buy time and barter the attackers down."(Systems Architect, BMI)

D. Exchanging threat information

Our extensive research on Generation IV ransomware incidents indicates that victims are extremely reluctant to confirm data breaches although there is clear evidence of them taking place. The reason the world is aware about these attacks is because hackers broadcast data breaches and post stolen information online (if a victim refuses to pay). One of the victims opined about this trend:

"I can tell you one of the things that really bothers me about security incidents is that organizations hide this information. But the more people keep this behind closed doors, the less we know. We are giving the advantage to the bad guys by not sharing this information. This is why we were so open about our breach" [Executive Manager, EducInstFB]

An interviewee from the aviation sector observed that:

"In air transport, we share every single piece of information about problems that we encounter ... but in InfoSec, we do almost the complete opposite."

Although knowledge about attacks is invaluable, the truth is that we know very little about the realities of ransomware attacks and their level of incidence. Managers often cover things up and reveal only paltry details in incident reports, which does not add to our knowledge on important facts of the incidents (e.g. attack vector, the methods used for lateral movement, reconnaissance details etc.). One of the police officers commented that:

"Generally, even companies that experience security breaches and call us to help are very squeamish about details of the incidents. They try to conceal details that can in any way place the finger of blame on them. It is a bit frustrating as we are trying to help." [Detective Sergeant, CyberBL].

Indeed, fear of adverse consequences remains a major barrier to information sharing. Organizations are potentially faced with huge fines and public persecution via broadcast, print and social media. Media exposure can be particularly hurtful when inaccurate facts are reported. As one of the interviewees from an affected organization commented:

"Media reports claimed that that we were being held to ransom for a 7-digit amount, which was not the case [the ransom for this victim was around £300 per machine and only a handful of machines were infected]. This damaged our reputation because of the adverse local and international coverage. And within half an hour of media exposure, I had five police officers on the doorstep because they thought we were subject to an ongoing live fraud or bribery. Security vendors then followed suit and printed information which was wrong and damaging to us. This was disappointing because we expected that security vendors would at least try and establish facts. As a result of this exposure, everyone was trying to get a hold of us, creating 'communication Wild West'. We were in the middle of a difficult recovery and this situation did not help us at all." [Security Manager, GovSecJN]

Indeed, such traumatic experiences can make victims reluctant to share incidents with the world:

"Excessive media attention hampered our recovery process because we were busy being pulled off to answer questions when we were actively trying to deal with the issue that was going on. It changed our attitude of how we would approach this in the future. I do not think we would be as forthcoming with that information, at least not directly to the press as we do right now." [Security Manager, LawEnfJ]

Nevertheless, the need to create shared platforms for security breaches is greater than ever before. One such initiative, the Cyber Security Information Sharing Partnership (CiSP), was organized by the National Cyber Security Centre (NCSC) in the UK to allow organizations share cyber threat information in a secure and confidential environment. This platform, however, is very selective about its members. It also contains many private groups that withhold information from the rest of the participants. Cyber threat information shared on CiSP thus lacks transparency and cannot be used for research to inform other interested parties about the most up-to-date threats. There is hence a need for a better mechanism to collect threat information. Such a platform should be fully anonymized, but at the same time transparent and universal in regard to access. The benefits of this initiative should be clearly articulated to victims of cybercrime to encourage sharing.

E. Emails and password hygiene

Phishing remains the most common ransomware attack vector [8]. Despite years of research into technical countermeasures to tackle phishing, including recent innovations in the areas of artificial intelligence, it remains a very serious problem. Spear phishing and business email compromise (BEC) attacks can sometimes be executed using very simple techniques that appear to be legitimate, such as impersonation and hi-jacking of trusted resources. Attackers may spend several months inside a network to build up a dossier of information about their victim. These types of attack are very difficult to prevent and detect using automated tools, and user education is the most effective strategy. Password hygiene remains a major problem in organizations [19]. Employees continue to use weak passwords, use the same passwords on several systems, or write them down. On the other hand, creating a spoof website that entices a user to enter their credentials does not require advanced technical skills. Therefore, hackers can easily obtain login information and even steal money, financial details, and personal data.

Police shared details of a case where an organization in the pharmaceutical sector ("PharmCo") became a victim of whaling. One of their executives received an email prompting to reset their Office 365 password, the instruction they regrettably followed. Attackers gained access to executive's credentials and set up rules that enabled them to intercept highly confidential data and commit financial fraud. Upon investigation, the external IT providers found that criminals stayed undetected inside PharmCo's network for about a month and swooped around SharePoint documents.

Email systems administrators should therefore deploy practices and procedures to counteract these potential threats. Enforcing multi-factor authentication and disabling email forwarding to external domains are two very simple steps that can be done. On many email services, these options are disabled by default, thus leaving the door open for an attacker to take advantage of laxity. Email forwarding to an external address should be red-flagged in the server security and compliance dashboard, and users should be prohibited from doing so unless explicit permission has been sought in exceptional circumstances for a limited period. Even if the external email address to which messages is forwarded is legitimate, or appears to be so, it should always be queried. It is very easy for an impostor to set up an email account on a "free" service using a false name to impersonate the actual owner. In particular, messages that have attachments or contain internal information that is of a confidential nature should not be permitted to be forwarded externally. The use of natural language recognition algorithms to process the content of email messages has ethical and legal issues but must be considered in light of the risk of sensitive data being leaked outside an organization. Internal email forwarding should also be carefully monitored because of the risk posed by rogue insiders [20] and also the possibility that a hacker is redirecting emails to an unmonitored internal account so as not to raise suspicion.

V. Conclusion

The fight against the continually evolving threat of ransomware is a constant game of cat and mouse, a battle of wits between attackers and defenders. Cybercriminals rely to a very large extent on methods that exploit inherent human weaknesses and tendencies. In order to fend off this menace, it is necessary to understand their modus operandi and to design systems and processes accordingly. In addition to having a solid grasp of potential technical exploits, it is just as important to understand how cybercriminals can cunningly avail of behavioral weaknesses to gain unauthorised access in unsophisticated ways that go under the radar.

Cybercriminals now spend a considerable amount of time conducting reconnaissance, both pre-attack and also after gaining entry. If a phisher succeeds in obtaining login credentials, he/she can penetrate a network, move laterally, and conduct internal reconnaissance by eavesdropping and rummaging through files. It is vital to beat intruders at their own game. Firstly, know what personal information about high-level managers can be found in the public domain and advise executives to be parsimonious about what they choose to reveal so as not to fall victim to whale and spear phishing. Secondly, know your data intimately, as is required by GDPR. Survey what assets are exposed on a device or network and regularly conduct internal reconnaissance scans, mimicking the types of hunting strategies that an attacker or rogue insider might use to probe for weaknesses in attempts to exfiltrate sensitive data. Thirdly, ensure appropriate information security controls on cloud-based environments. Fourthly, get the basics right: practice good email hygiene and have well rehearsed incident response plans in place so that if an attack strikes at an inopportune moment, employees are not flailing and floundering and know precisely what to do to limit damage. Finally, consider that no technology offers a 'silver bullet' – implementing an array of controls, hence, is paramount.

We leave the final word to a senior police officer who we asked to review our recommendations. He advises that:

"If attacked, network segregation is extremely important to mitigate the impact of hybrid ransomware. Organizations should utilise an array of services and continually check advice from the likes of UK NCSC. I cannot emphasise enough the importance of employee training and strong password mechanisms, including the implementation of multiple-factor-authentication, especially external facing services. I strongly recommend investing time into mitigation and recovery mechanisms. Cryptocurrencies are the currency of choice for cyber criminals and have been a significant factor affecting the proliferation of ransomware. Without ready access to cryptocurrency assets to pay demands, victims can be afforded a reasonable period of time in which they can work to report, mitigate and recover whilst considering their options with regards to payment."

References

[1] Sophos, "The State of Ransomware 2020: Results of an independent survey across 26 countries"; https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

[2] L. Connolly and D. Wall, "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures", *Computers & Security*, vol. 87, 2019, pp. 1-18.

[3] D. M. Nicol, "The Ransomware Threat to Energy-Delivery Systems", *IEEE Security & Privacy*, vol. 19, no. 3, 2021, pp. 24-32.

[4] K.S. Choi, T.M. Scott and D.P. LeClair, "Ransomware against police: diagnosis of risk factors via application of cyber-routing activities theory", *International Journal of Forensic Science & Pathology*, vol. 4, 2016, pp. 253-258

[5] J.Y. Zhao et al., "Impact of trauma hospital ransomware attack on surgical residency training", *Journal of Surgical Research*, vol. 232, 2018, pp. 389-397.

[6] L. Zhang-Kennedy et al., "The aftermath of a cryptoransomware attack at a large academic institution". *Proceedings of 27th USENIX Security Symposium*, 2018, pp. 1061-1078.

[7] L. Connolly et al., "An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability", *Journal of Cybersecurity*, vol. 6, no. 1, 2020, pp. 1-18.

[8] Coveware, "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands", 1 February, 2021; https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

[9] Coveware, "Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase", 3 August, 2020; https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report

[10] Information Commissioner Office (ICO), 2020; https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/

[11] B. Malik, "Cognizant's net profit down 29 per cent in Q2, 2020 due to ransomware attack, COVID impact", *The New Indian Express*, 30 July, 2020; https://www.newindianexpress.com/business/2020/jul/30/cognizants-net-profit-down-29-per-cent-in-q2-2020-due-to-ransomware-attack-covid-impact-2176847.html

[12] K. Dwyer, "It's 2020 and Only 20% of Companies Are Ready for a Ransomware Attack", *Risk & Insurance*, March 10, 2020; https://riskandinsurance.com/its-2020-and-only-20-of-companies-are-ready-for-a-ransomware-attack/

[13] J.P. Mello, "8 lessons from the Garmin ransomware attack", 2020; https://techbeacon.com/security/8-lessons-garmin-ransomware-attack

[14] University of California San Francisco (UCSF), "UC part of nationwide cyber attack", 31 March, 2020; https://ucnet.universityofcalifornia.edu/news/2021/03/uc-part-of-nationwide-cyber-attack.html

[15] I.C. Palli, "REvil Ransomware Gang Auctioning Off Stolen Data", June 3, 2020; https://www.bankinfosecurity.com/revil-ransomware-gang-auctioning-off-stolen-data-a-14378

[16] J. Tidy, "Hackers threaten to leak plastic surgery pictures", *BBC News*, 24 December, 2020; https://www.bbc.com/news/technology-55439190

[17] A. Kharraz et al., "Protecting against Ransomware: A New Line of Research or Restating Classic Ideas?", *IEEE Security & Privacy*, vol. 16, no. 3, 2018, pp. 103-107.

[18] Hiscox; "Data exfiltration during ransomware attacks"; https://www.hiscox.co.uk/sites/uk/files/documents/2020-07/20816-Data-exflitration-guide-final.pdf

[19] G.C. Jayakrishnan et al., "Password: A serious game to promote password awareness and diversity in an enterprise", *Proceedings of 16th Symposium on Usable Privacy and Security*, 2020, pp. 1-18.

[20] S. Browne, M. Lang, and W. Golden, "The insider threat: understanding the aberrant thinking of the rogue trusted agent", *Proceedings of 23rd European Conference in Information Systems*, 2015, pp. 1-11.

Table 1. Evolution of ransomware

Generation, Year of emergence	**Infection extent**	**Attack outcome**	**Threat description**	**Location of apprehended data**
I, 1989	One machine (sometimes only selected parts of the machine)	Data encrypted with weak cryptographic algorithms	Extortion	Victim's network
II, 2013	One machine and certain devices that are physically (e.g. external drive) and logically (e.g. server shares) connected to the infected machine	Data encrypted with virtually unbreakable cryptographic algorithms	Extortion	Victim's network
III, 2016	Entire networks	Data encrypted with virtually unbreakable cryptographic algorithms	Extortion	Victim's network
IV, 2019	Entire networks	Data encrypted with virtually unbreakable cryptographic algorithms and stolen, and data exfiltrated	Extortion and blackmail	Victim's network and other attacker-controlled location