Threat Landscape Snapshot

Retail

March 2020

Cyberint

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The retail industry is subject to attack from 'all angles' and was the third most targeted industry worldwide in 2019, as observed in Cyberint's CiPulse 2020 Threat Landscape report (Figure 1).

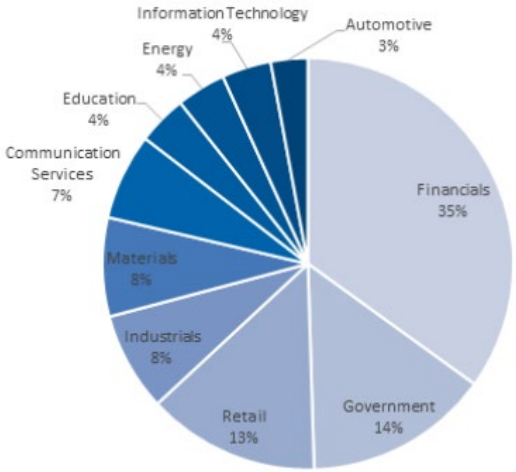

Figure 1 - Industries under attack in 2019

With internet-based sales increasing year-on-year (Figure 2), coupled with the ongoing digitization of our daily lives, it is unsurprising that financially motivated threat actors of varying sophistications continue to target the potentially lucrative retail industry.

Figure 2 - Internet sales as a % of total retail sales [Source: UK Office for National Statistics]

Further compounding the threats to retailers in the first quarter of 2020, the global outbreak of the COVID-19 pandemic has increased demand for online retailers, especially with government-imposed restrictions on movement, increased work-from-home activity and potential staff shortages due to illness or 'self-isolation'.

Taking advantage of this somewhat perfect storm, threat actors, both cybercriminal and nation-state sponsored, have been crafting campaigns that leverage the worldwide concern and anxiety, utilizing COVID-19 themed lures to deliver malicious payloads.

As many individuals and organizations struggle to maintain a sense of normality in these times, there is no apparent let up in malicious activity. Given this, the retail industry, much like many other industries, needs to maintain a solid cybersecurity posture and adapt to the ongoing challenges.

Key Findings

- COVID-19-themed lures are understandably prevalent at this time,
- Targeted ransomware attacks have increased throughout 2020 and employ a ‘steal, encrypt and leak’ tactic along with victims being 'named and shamed' on threat actors' websites,
- COVID-19-themed ransomware has also been observed,
- Credential stuffing remains a favored attack method against retailers and online service providers for low-sophistication threat actors,
- Skimming attacks against online ecommerce platforms continues to be prevalent with a reported two million websites infected during 2019.

THREATS & THE THREAT LANDSCAPE

COVID-19-THEMED LURES

Many cyberattacks commence with the delivery of an email lure that typically uses language and terminology to encourage the recipient to open a malicious attachment or click on a malicious link. Whilst many will be accustomed to these types of threat, there has been a sharp rise in the number of COVID-19 themed lures (Figure 3) sent by threat actors throughout March 2020.

Figure 3 - Example COVID-19 themed email lure

As both retail industry employees and customers seek up-to-date information on the pandemic, lures of this nature may appear very convincing, especially given the volume of legitimate COVID-19 related emails being received at this time. Furthermore, with many people working from home and being subjected to differing stresses at this time, cybersecurity awareness is unlikely to be at the forefront of their minds and many will therefore be susceptible to this nefarious activity.

In addition to email-based threats, domain registrations using the keywords 'Corona' or 'COVID', many of which are undoubtedly for nefarious use, have massively increased since the beginning of 2020 and month on month so far (Figure 4).

With an average of over 2,300 domains being registered per day during March 2020, this is a massive increase of some 636% compared to domain registrations using the same keywords in February 2020. Furthermore, based on risk scores assigned by DomainTools®, 86% of these keyword domains registered in March 2020 are classified as high risk, that being domains that are known bad due to spam, phishing or malware and domains that are hosted in close proximity to known nefarious content.

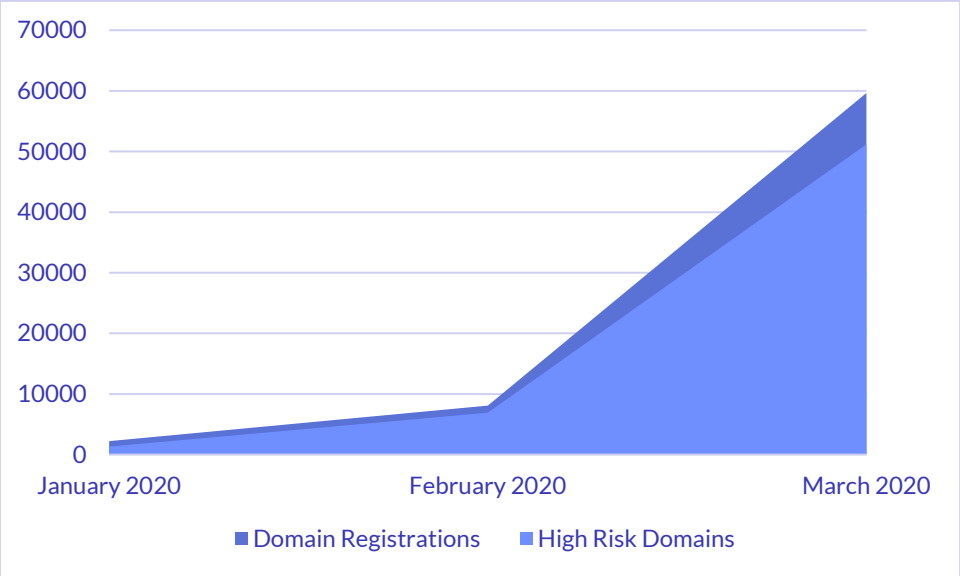

Figure 4 – 'Corona' and 'COVID'-related domain registrations and proportion of high risk domains

Aside from commodity malware being distributed via COVID-19 themed campaigns, such as remote access trojans and password stealers, nation-state threat actors have been linked to attacks against government, health and pharmaceutical targets, likely in an attempt to gather intelligence for use in their own responses to the ongoing issue.

Whilst the retail industry may not be a direct target of these nation-state attacks, financially motivated threat actors will seize upon any opportunity to gain a foothold in potentially lucrative targets and if employees, especially those working from home, fall victim to these campaigns their corporate credentials could be compromised and later abused.

Further compounding the situation, threat actors may seek to exploit high-traffic websites to deliver malicious payloads to visitors. One such recent example of this was the apparent use of the U.S. Department of Health & Human Services (HHS) website, a site likely visited by countless Americans seeking public health updates, as a redirect to malicious infrastructure hosting an information stealer (Figure 5).

```
https://dcis.hhs.gov/cas/login?service=http%3A%2F%2F195.130.73.229/php/hhs/&gateway=true
```

Figure 5 - US HHS Website redirection to malicious infrastructure

In this instance, the information stealer payload was a malware-as-a-service (MaaS) threat named 'Raccoon' that has previously been available for as low as US$75 per week or US$200 per month. Once deployed, the stealer targets login credentials, payment card data, cryptocurrency wallets and browser information from over sixty different applications, exfiltrating these via HTTP POST requests to the threat actor's infrastructure for later abuse.

RECOMMENDATIONS

- Employee security awareness training is now, likely more so than ever, an important step in ensuring that those on the front line are able to spot and stop attacks in their tracks. As many

employees work from home or adapt to increased online habits, they should be reminded to be suspicious of any unsolicited or unusual communication and, when seeking information related to the ongoing COVID-19 situation, stick to known official sites.

- Where possible, access to new and low reputation websites should be denied to prevent employees from accessing new and emerging threats as well as preventing 'call home' type activity from compromised machines that may have thematic command and control (C2) domains. The use of thematic domains can be utilized to avoid suspicion from analysts when reviewing logs containing both legitimate and nefarious activity.

- As with any email-based threat, robust email gateway controls can prevent malicious, suspicious or unsolicited messages arriving in mailboxes. In addition to verifying the reputation and validity of the sender's domain and IP address, message attachments and embedded URLs, where present, should be scanned for malicious content and the message either deleted or quarantined depending on the outcome. Given the potential for COVID-19 related lures at this time, consideration should be given to quarantining messages with COVID-19 themed subjects, message bodies and attachments if the sender origin cannot be reliably confirmed as legitimate.

- Policies such as DMARC (Domain-based Message Authentication, Report and Conformance) can be used to validate messages and thwart email spoofing as observed in recent COVID-19 themed campaigns masquerading as sent from the World Health Organization (WHO). DMARC, as detailed in RFC7489 , provides a mechanism for the sender domain to advertise their use of DKIM (Domain Keys Identified Mail) and/or SPF (Sender Policy Framework), allowing the recipient to validate a message, receive feedback of domain abuse and specify the receiver action should the message fail authentication.

- When sending legitimate communications to customers, retailers should consider personalizing emails, such as addressing customers by their full name or including partial elements of their personal data, as well as advising them on the nature of legitimate communications sent, for example, advising customer that they will never be asked for payment information or passwords via email. Furthermore, customers should be reminded not to submit or surrender personal information without directly visiting the legitimate retailer's website.

CREDENTIAL STUFFING

Readily available ‘account checker' tools and configuration files ensure that credential stuffing remains a credible threat to both retailers and online service providers.

These tools allow low-sophistication threat actors to bulk test credentials, typically obtained from data breaches or leaks, against a variety of online retailers and services to identify customers that have reused the same credentials across multiple services. Once a successful combination of credentials has been found, the tools typically extract pertinent account information such as details of any credit balance or subscription status (Figure 6) and then log this for later abuse by the threat actor.

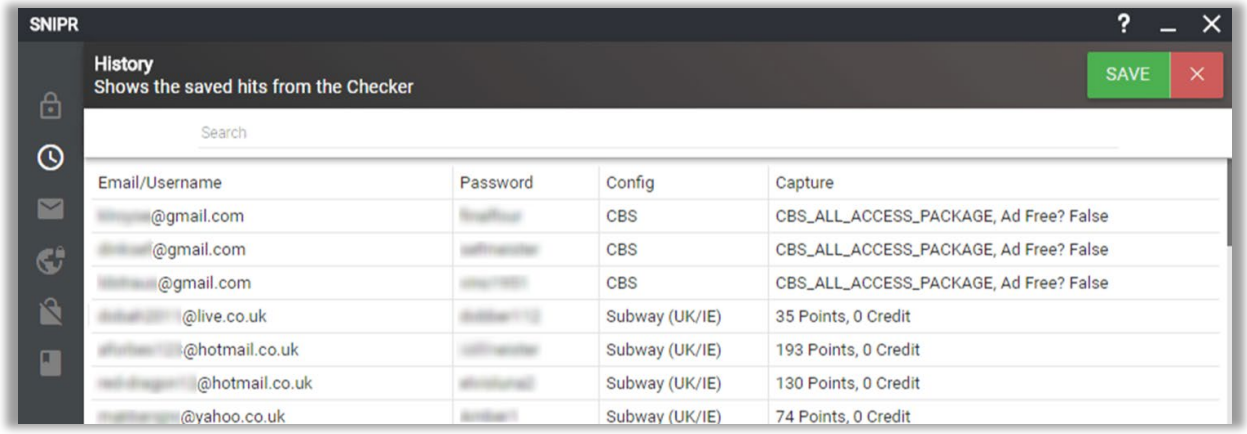

Figure 6 - Credential stuffing tool

Credential leaks, commonly referred to as 'combos', are commonly traded on underground forums and marketplaces and therefore these attacks require little more than downloading the tool, a retailer or service specific configuration and a ready-made 'combo' list. To avoid automated detection, many tools also support the use of proxies and the threat actor will typically need to compile a list of proxy servers, again freely available, that are cycled through for each authentication attempt.

Subsequent abuse of compromised accounts can include the extraction of payment card data, if not properly secured or obfuscated by the service, theft of credit or gift card balances, and the fraudulent acquisition of goods and services.

In the latter case, fraudulent transactions would often involve the purchase of digital goods, such as gift cards or subscriptions, as these can often be used somewhat anonymously anywhere in the world and are easy to resell or trade. Conversely, fraudulent transactions involving physical goods would likely require the threat actor to be located in the same region as the victim customer as well as needing a 'drop' address to receive the goods.

RECOMMENDATIONS

- Given that the success of credential stuffing attacks relies on poor credential hygiene, specifically the reuse of credentials across multiple sites or services, both employees and customers should be reminded to use unique passwords for each service.
- Additional controls such as multi-factor authentication (MFA) will thwart credential stuffing attacks as, even if credentials are reused, the threat actor would not have access to the token or device used by the customer. Furthermore, adding additional steps into the authentication process, such as requiring the customer to confirm known details or complete an anti-bot countermeasure such as a 'CAPTCHA', may also thwart automated attacks.
- Steps can also be taken to potentially identify anomalous behavior including the blacklisting of connections from known proxies, VPN nodes or anonymization networks, especially as legitimate customers are unlikely to use these services. Furthermore, automated attack tools may have specific behavioral signatures in the way that they attempt to access services, as such these may enable them to be detected and blocked by web-application firewalls or other countermeasures.

SKIMMING ATTACKS

Both online payment processing and physical point of sale (POS) systems continue to be lucrative compromise points for financially motivated threat actors targeting the retail industry.

Following a reported compromise of some two million websites in 2019, digital skimming attacks against online retailers, such as those conducted by the various 'Magecart' threat groups, remain current in 2020 with customer payment data being stolen during the 'checkout' process (Figure 7).

Figure 7 - Online shopping/skimming process

Whilst these skimming attacks typically involve the compromise or code injection of a retailer's ecommerce platform, previous campaigns have seen third-party services being compromised, such as advertisers or web-analytic providers, so that malicious code is loaded alongside the embedded third-party code on the retailer's website.

In addition to appending malicious script code onto legitimate ecommerce pages and scripts (Figure 8), previous campaigns have also seen malicious scripts being hosted on the threat actor's infrastructure, sometimes mimicking domains that are similar to the target retailer, with simple 'script' tags being injected into the retailer's website (Figure 9).

```
function validateCreditCard(s) {
    // remove non-numerics
    var v = "0123456789";
    var w = "";
    for (i=0; i < s.length; i++) {
        x = s.charAt(i);
        if (v.indexOf(x,0) != -1)
        w += x;
    }
    // validate number
    j = w.length / 2;
    k = Math.floor(j);
    m = Math.ceil(j) - k;
    c = 0;
    for (i=0; i<k; i++) {
        a = w.charAt(i*2+m) * 2;
        c += a > 9 ? Math.floor(a/10 + a%10) : a;
    }
    for (i=0; i<k+m; i++) c += w.charAt(i*2+1-m) * 1;
    return (c%10 == 0);
}
```

```
T7Qq.d6Sf=function (){return typeof T7Qq.Z6Sf.V3==='function'?
T7Qq.Z6Sf.V3.apply(T7Qq.Z6Sf,arguments):T7Qq.Z6Sf.V3;};T7Qq.R6Sf=function (){return typeof T7Qq.Z6Sf.g2==='function'?
T7Qq.Z6Sf.g2.apply(T7Qq.Z6Sf,arguments):T7Qq.Z6Sf.g2;};T7Qq.b5zM=function (){return typeof T7Qq.y5zM.g2==='function'?
T7Qq.y5zM.g2.apply(T7Qq.y5zM,arguments):T7Qq.y5zM.g2;};T7Qq.m7wX=function (){return typeof T7Qq.N7wX.s1==='function'?
T7Qq.N7wX.s1.apply(T7Qq.N7wX,arguments):T7Qq.N7wX.s1;};T7Qq.F7wX=function (){return typeof T7Qq.N7wX.o2==='function'?
T7Qq.N7wX.o2.apply(T7Qq.N7wX,arguments):T7Qq.N7wX.o2;};T7Qq.K5zM=function (){return typeof T7Qq.y5zM.g2==='function'?
T7Qq.y5zM.g2.apply(T7Qq.y5zM,arguments):T7Qq.y5zM.g2;};T7Qq.d7wX=function (){return typeof T7Qq.N7wX.g2==='function'?
T7Qq.N7wX.g2.apply(T7Qq.N7wX,arguments):T7Qq.N7wX.g2;};T7Qq.Z6Sf=function(s6Sf){return{g2:function(){var
O6Sf,N6Sf=arguments;switch(s6Sf){case 16:O6Sf=(N6Sf[1]&N6Sf[0])<<N6Sf[5]-N6Sf[4]|N6Sf[2]&(N6Sf[6]|N6Sf[3]);break;case
10:O6Sf=N6Sf[1]>>+N6Sf[2]|+N6Sf[0];break;case 3:O6Sf=N6Sf[1]>>+N6Sf[0];break;case 7:O6Sf=N6Sf[1]
```

Figure 8 - Malicious code appended to legitimate code

Figure 9 - Malicious code hosted on the threat actor's infrastructure

Once compromised, these malicious skimmer scripts allow the threat actor to record any information entered by the customer into forms during the online checkout process, including their personal details and full payment card information.

RECOMMENDATIONS

- Given that many of these attacks rely on compromising ecommerce platforms, it is imperative that both the webserver and any platform or development frameworks are regularly updated to patch security vulnerabilities that could permit unauthenticated access or code injection.
- The use of Content-Security-Policy (CSP) on webservers can allow a list of trusted locations, from where resources can be loaded, to be defined and prevent malicious scripts hosted on third-party domains from being executed. Furthermore, logging and reviewing CSP violations may serve as an early warning of malicious activity.
- When accessing and loading resources from trusted third-parties, Sub-Resource Integrity (SRI) checking allows the browser to verify that the content fetched has not been manipulated or modified by performing validation against a cryptographic hash of the original content.

TARGETED RANSOMWARE

Although mass indiscriminate ransomware campaigns were in decline throughout 2019, 2020 has seen an increase in sophisticated and targeted ransomware attacks against organizations in all industries.

Differing from traditional ransomware campaigns, focused on only encrypting data to extort a ransom payment, these campaigns typically involve the compromise of the target network, such as through the exploitation of zero-day vulnerabilities, the theft of sensitive data including IT infrastructure documentation, customer records, and payment card data, and then finally the encryption of systems. Subsequently, the threat groups behind these targeted ransomware campaigns demand payment for both the decryption of the affected systems as well as to prevent stolen data from being publicly leaked.

This 'steal, encrypt and leak' tactic first appeared to be used by predominately Russian-speaking ransomware groups in November 2019 and has since been adopted by numerous other groups to great effect. These threat groups understand the consequences of their actions and stress to victims the

importance of paying their ransoms versus the potential cost arising from an incident becoming public knowledge, be that regulatory and legal penalties or decreased customer confidence and reputational damage. To apply further pressure, sample sets of stolen data have been leaked at intervals (Figure 10) and this data has previously included information that could easily be abused by other threat actors in additional attacks against the victim.

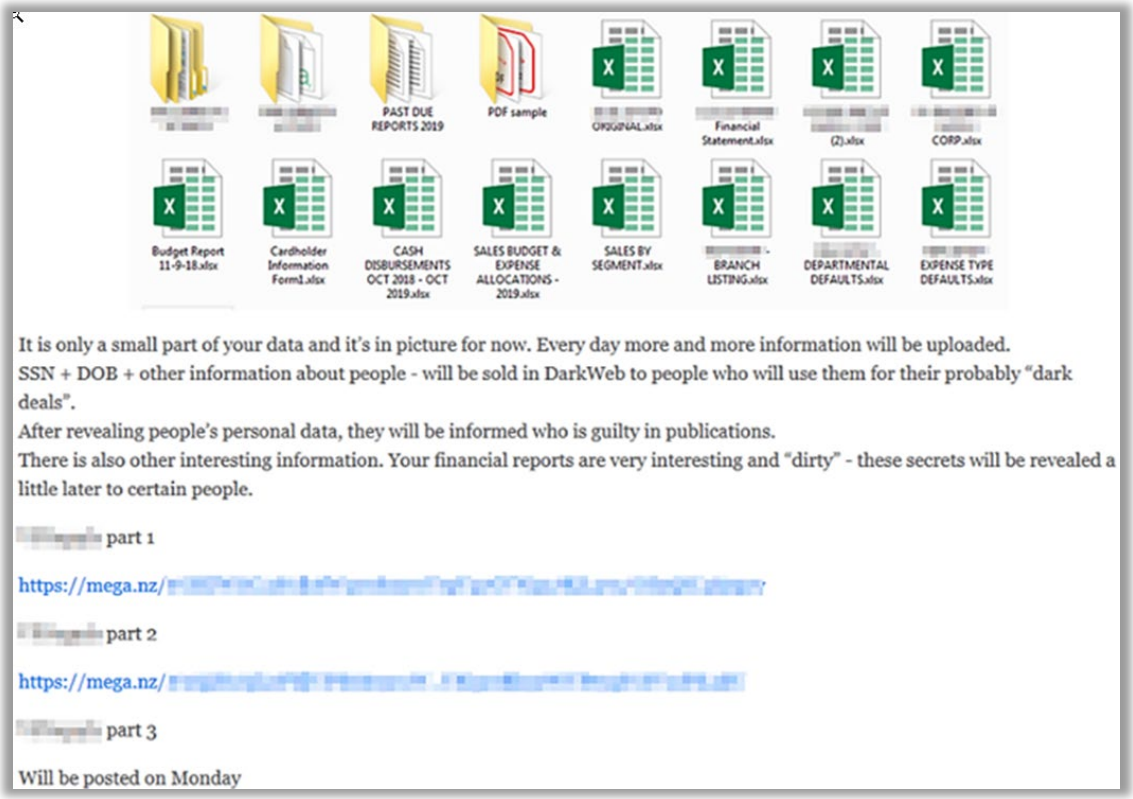

Figure 10 - Example stolen data leak

Organizations targeted by these ransomware threat groups have varied in both size and sector, from the widely publicized Travelex incident over the New Year period to a group of dental surgeries and various industrial facilities. Typically, targeted organizations are those that have high value assets and a high net worth although perhaps not organizations that are so large that they would be heavily defended. This method of selecting victims that have the capability to pay high value ransoms has been dubbed 'big game hunting' and, aside from those with sufficient cash flows, organizations with cyber insurance policies make 'good' targets that are likely to pay their ransom demands quickly.

Organizations operating within the retail industry, whilst seemingly not heavily targeted thus far, would make desirable targets for targeted ransomware attacks, especially given the potential for loss of earnings and customer confidence if ecommerce platforms are taken offline for any period of time. This situation would be further exacerbated by the current COVID-19 situation with many customers relying on the ability to place online orders given the widespread restrictions on movements and store closures worldwide.

Further embarrassing the victims of these targeted ransomware attacks, many of the threat groups have shifted from sharing details of their victims on closed cybercrime forums to creating and posting on publicly accessible websites. These 'naming and shaming' websites (Figure 11) are, given their public nature, frequented by security researchers and journalists alike, resulting in news of victims becoming public knowledge much faster.

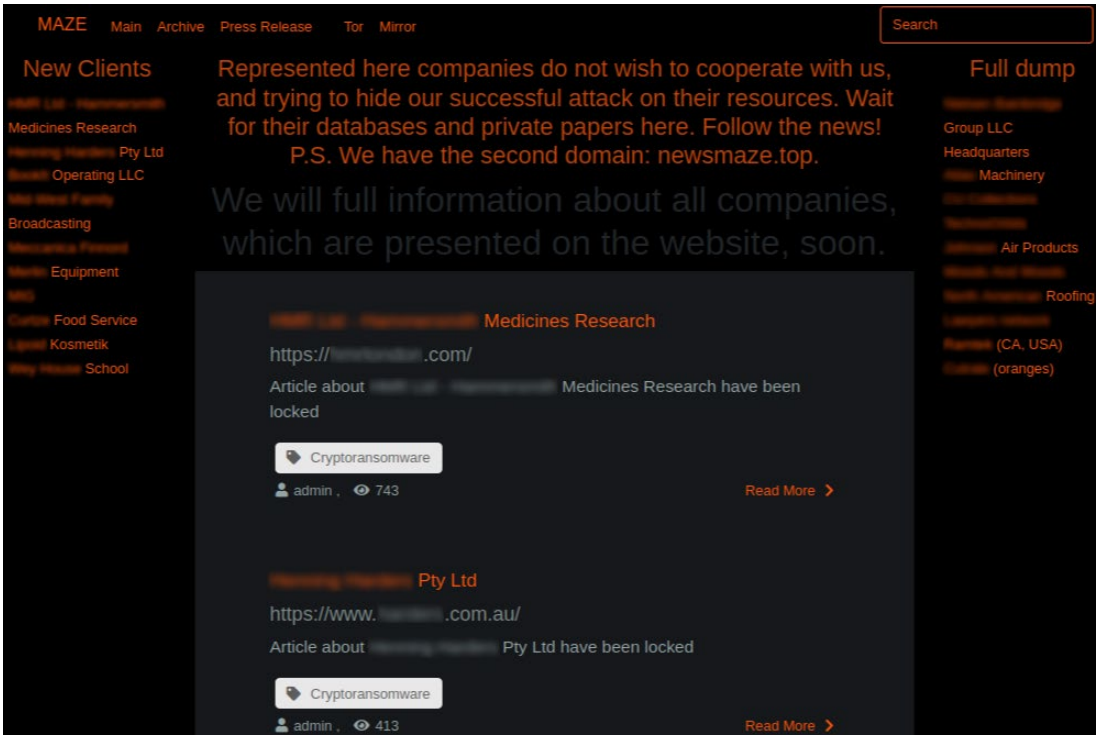

Figure 11 - Example ransomware group 'name and shame' website

Worse still, it appears, based on a post shared on one of these websites, that those that have paid ransoms may still be named and shamed (Figure 12), albeit in this case the retail fashion house victim may have ignored earlier, somewhat private, ransom demands.

Figure 12 - Details of paying victim shared by the threat group

As is to be unfortunately expected during this ongoing global public health situation, ransomware threats have also started to utilize COVID-19 themes in their email lures as well as 'new' ransomware

variants being released such as the 'Coronavirus Ransomware' (Figure 13) and 'CovidLock', an Android App that locks a victim's smartphone.

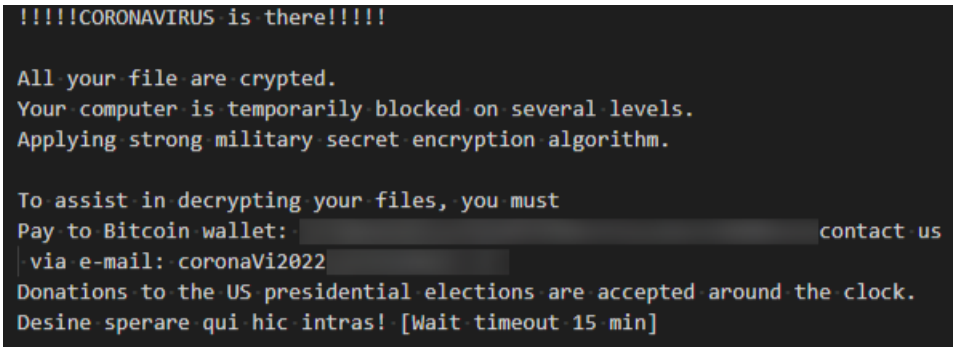

Figure 13 - 'Coronavirus Ransomware' encryption note

RECOMMENDATIONS

- Whilst the majority of these ransomware attacks commence with a network intrusion, employees should still be aware and suspicious of unsolicited emails containing attachments or links as this method of initial compromise may still be leveraged by some threat actors.

- Based on publicly available information following some of the high-profile targeted ransomware attacks thus far this year, many initial network intrusions have exploited known vulnerabilities in internet-facing services, including RDP servers and VPN nodes. Given this, organizations should ensure that systems are regularly updated to ensure that known vulnerabilities are patched and their attack surface reduced.

- Leaked data from numerous victims has included IT infrastructure documentation including credentials within files that can subsequently be abused and used to compromise further systems. Given this, sensitive data should always be adequately encrypted and stored securely to prevent unauthorized access, even in the event of the file being stolen.

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
14 Grays Inn Rd, Holborn, WC1X 8HN, London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +507-395-1553
Panama City