CORVID
Intelligent Cyber Defence

CORVID

COMPANY 1
COMPROMISE ASSESSMENT REPORT

CORVID ref: Cy1/2018/14

Date: 4 September 2018

www.corvid.co.uk

Please note: This redacted report is an example of a CORVID Compromise Assessment. As the service is tailored to each customer's requirements, this only shows a sample of our capability.

CONTENTS

INTRODUCING CORVID

CORVID is a government-grade solution for managed cyber defence with a proven experience of defeating attacks from state sponsored sources and criminal gangs. CORVID analyses artefacts used by adversaries which are undetectable by anti-virus.

CORVID was developed by Ultra Electronics, a FTSE 250 company. Ultra Electronics was founded in 1920 and has spent the last 20 years providing smart electronics technology for the aerospace and defence industries. Typically, Ultra technology is used to safeguard military, aerospace and critical infrastructure technologies. Ultra's pedigree enabled it to identify that traditional cyber-defences were insufficient to combat the evolving complexity of threats. Hence the CORVID initiative was started to provide a better and more comprehensive solution to the cyber problem. At the request of suppliers and business partners, it was decided to make CORVID available as a commercial solution to all organisations.

INTELLIGENT CYBER DEFENCE

Our approach to IT security is intelligence led; we combine internally generated intelligence with other sources and take an active approach to malware detection, hunting down the latest threats and constantly monitoring for evidence of compromise.

At CORVID we have a simple set of questions to judge whether an organisation is cyber-secure.

a. How many attacks hit your boundary each month?

   This is an essential statistic. In the physical world it is easy to assess whether you live in a hostile neighbourhood. You need to be able to make the same assessment of your digital neighbourhood. It is impossible to make an informed decision without the right information.

b. If malware is detected, do you receive a report detailing how long it has been there and what it has done?

   When an attacker has been present within your systems you should identify the following:

   - How they got in
   - What was stolen
   - How to clean up
   - How to make sure it doesn't happen again

It is not possible to understand the cost of an attack without understanding the nature of the attack.

EXECUTIVE SUMMARY

This report summarises the Compromise Assessment conducted by CORVID on the IT infrastructure of Company 1 (Cy1) between Monday 30 July 2018 and Friday 31 August 2018.

Based solely upon the analysis of the data generated during the Compromise Assessment, CORVID would consider that Cy1's IT systems currently have a good level of cyber hygiene. Analysed artefacts would suggest that there is not an active compromise present within the Cy1 estate.

However, the Assessment did discover some areas of concern including the discovery of artefacts that suggest one host may have been compromised in 2015, two Potentially Unwanted Programs (PUPs) installed on four hosts, and installations of outdated software that is commonly targeted by attackers. To reduce the risk of future compromise, CORVID recommends that the identified areas be addressed at the earliest opportunity.

FINDINGS SUMMARY

SERVICE	ANALYSIS AREA	FINDING(S)	
PICA	Persistence Analysis	Whilst no evidence of active advanced persistent malware was discovered, artefacts that suggest one (1) host may have been compromised in 2015 was found.	
PICA	Potentially Unwanted Program (PUP) Analysis	Two (2) notable PUPs installed on four (4) hosts were discovered.	
PICA	"Shadow IT" Software	Potential "Shadow IT" software discovered.	
PICA	Process Analysis	No evidence of active malware was identified.	
PICA	PowerShell Analysis	Whilst no evidence of malicious PowerShell usage was discovered, four (4) hosts were identified as having a non-standard Execution Policy.	
PICA	File Analysis	No evidence of dormant malware was discovered.	
PICA	Event Log Analysis	No evidence of suspicious activity was discovered.	
PICA	Lateral Movement Analysis	No evidence of suspicious lateral movement was discovered.	
PICA	Administrative Privileges Analysis	Administrative Privileges review recommended.	
PICA	Known Attack Campaign Analysis	No evidence of compromise from known attack campaigns was discovered.	
CORAX	Known Bad Domain Analysis	No communication with high confidence known bad domains was discovered.	
CORAX	Advanced Command & Control Malware Analysis	No evidence of active advanced command & control malware was discovered.	
CORAX	Beacon Malware Analysis	No malicious beacons were discovered.	
VARIS	Vulnerability Scan	2,880 High Severity vulnerabilities were discovered, including installations of outdated software that is commonly targeted by attackers.	

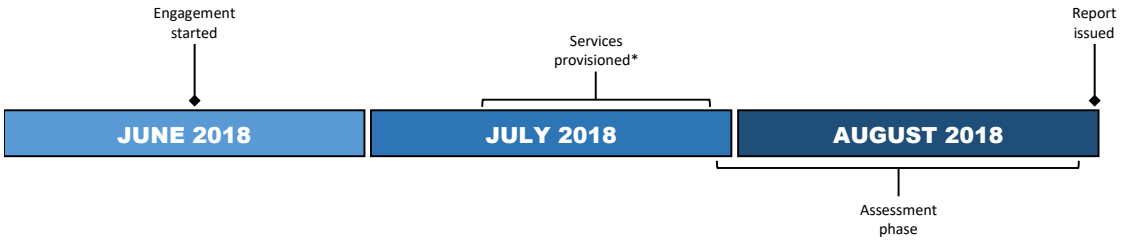
CYBER HEALTH

 **GOOD**	Evidence of legacy compromise discovered	**Staying Healthy:**
	No Targeted Attacks	**1)** Apply missing software patches to make Cy1 a harder target by reducing the attack surface
	PUPs and vulnerable software discovered	**2)** Conduct a review of administrative privileges to ensure that users are running with the least privileges possible to complete their job role

CORVID would like to thank Cy1 for permitting and supporting the Assessment that took place. Comments or further discussions on any aspect of this report would be welcomed.

THE IMPLEMENTATION

The assessment was performed on a single network and targeted 690 hosts. The CORVID service was provisioned during July 2018. The assessment commenced on Monday 30 July 2018 and concluded on Friday 31 August 2018.



ASSESSMENT SERVICES

The following CORVID service was selected to provide a continuous comprehensive assessment:

CORAX
INTERNET SECURITY

The CORAX service constantly analyses your Internet metadata for signs of compromise. Events of interest are reviewed by trained CORVID specialists. CORAX protects your company from some of the most prevalent threats on the Internet today; that could include: - “Ransomware”, “Exploit Kits”, and other families of malware.

VARIS
VULNERABILITY SCANNING

The VARIS service is a pro-active vulnerability scanning solution that reduces the opportunity for attackers to assess systems and restrict what they can do if they manage to get in. VARIS scans across an entire IT system to: identify vulnerabilities, understand them and assist with learning how to minimise the risk of attack.

PICA
MALWARE HUNTING

The PICA service provides advanced malware detection over and above what can be achieved by traditional anti-virus alone to find malware that is specifically targeting companies. PICA can restrict the window of opportunity of an attacker from months down to hours, dramatically reducing the damage that can be done to your company following a compromise.

PICA ASSESSMENT

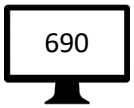
Despite the fact that 65% of publicly reported data breaches occur on endpoints (laptops, desktops, servers, etc.), many organisations still prioritise the wrong protection techniques across their environment. They focus on networks that are increasingly difficult to secure with large numbers of employees operating outside of them.

Time is the key factor in detecting compromise because intruders rarely execute their entire mission in the course of a few minutes, or even hours. In fact, the most sophisticated intruders often persist for months or years at a time. This window of time, from initial unauthorised access to ultimate mission accomplishment, gives defenders an opportunity to detect, respond to, and contain intruders before any damage is done.

PICA is a CORVID service that undertakes a daily analysis of endpoints, actively looking for signs of compromise and malware. It uses a bespoke agent that sits quietly on the host without interfering with any computer operations. This analysis is undertaken by security experts, rather than by a heuristic engine that can be emulated and defeated by the sophisticated attackers that are becoming more active on the Internet. The PICA service can reduce the window of opportunity of an attacker from months down to hours, dramatically reducing the damage that can be done to an organisation.

PICA ANALYSIS SUMMARY

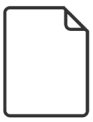
HOSTS ANALYSED



NUM. CHECKS CONDUCTED

91,305 (132 per host)

UNIQUE FILES ANALYSED



2,182,304 files

PERSISTENCE ANALYSIS

For an attacker to maintain a foothold inside your network, they will typically install a piece of backdoor malware on at least one of your systems. The malware needs to be persistent, meaning that it will remain active even after a reboot.

PICA has comprehensive knowledge of auto-starting locations and is able to detect those programs that are configured to run during system bootup or login. These programs and drivers include applications in your startup folder, Run, RunOnce and other Registry keys.

PICA extracts and processes information from every place in the system that can be configured to run something at boot and logon, including:

- Standard run keys and startup folders
- Shell, userinit
- Services and drivers
- Tasks
- Winlogon notifications
- Explorer addins

During the Compromise Assessment, two suspicious scheduled tasks ("AT jobs") were found on host HOST047. The AT jobs were created and last executed on 15th July 2015, and the referenced binary (sysins.exe) is no longer resident on the host. Following the discovery of this activity, sweeps were conducted and no similar artefacts were found across all other Cy1 hosts.

If Cy1 is unaware that HOST047 was previously compromised, CORVID recommends that an Incident Response investigation takes place to determine if Cy1 data was accessed by a threat actor.

No further evidence of advanced persistent malware was discovered to be present on Cy1's IT infrastructure.

POTENTIALLY UNWANTED PROGRAM (PUP) ANALYSIS

Unnecessary and unwanted software increases an organisation's attack surface and exposes systems to additional threats. A compromise of the Ask Partner Network (APN) infrastructure (https://www.scmagazine.com/ask-partner-network-compromised-again-to-spread-malware/article/645637/) gives an example of how attackers are exploiting the continued ubiquity of Potentially Unwanted Programs (PUPs) to conduct sophisticated attacks against enterprise networks.

Although not necessarily malicious by design, instances of PUPs can dramatically increase an organisation's attack surface and expose systems to additional threats. Often bundled with other freeware, common examples include browser toolbars and add-ons.

The primary purpose of most PUPs is to generate revenue; this is often achieved by injecting advertisements (browser hijacking), or by collecting and selling user search data. Functionality varies considerably, but many exhibit behaviour similar to malware, including:

- The ability to covertly install additional software
- Modification of browser search results
- Modification of system configuration
- Exfiltration of data including browser history, usage patterns and system configuration

The link above provides a good illustration of the weaknesses that can be introduced through PUPs. Sophisticated attackers successfully compromised the APN update mechanism, allowing them to deliver and execute digitally signed malicious payloads, therefore gaining full remote access to victim hosts. Furthermore, as many PUPs are installed as Windows Services, any compromise of the application often results in SYSTEM privileges being inherited.

In the same way that administrators should harden systems by disabling services that are not required, CORVID would encourage Cy1 to consider removing any third-party software that is not required to meet a business need. Additionally, although most anti-virus solutions will reliably detect PUPs, typically, the default configuration is such that PUPs will not be blocked/deleted (i.e. the AV software will warn only). CORVID encourages Cy1 to review their anti-virus configuration to ensure that maximum value is realised.

Finally, in light of the fact that some PUPs require administrative privileges to install, user permissions should be reviewed to prevent unauthorised software installation wherever possible. Although installing browser extensions/add-ons may not require administrative privileges, flexible configuration (such as preventing unauthorised extensions) is possible with most major web browsers.

NOTABLE PUPS DISCOVERED

The aforementioned analysis techniques (persistence, process and file) revealed a number of resident PUPs across Cy1's IT infrastructure. CORVID encourages Cy1 to consider removing the following software, providing it is not required to meet a business need:

PUP	DESCRIPTION	HOST(S)
MyWebSearch toolbar	MyWebSearch by MindSpark is a browser add-on that is known to hijack the browser, changing the search engine to one provided by MindSpark.	HOST142 HOST183
ASK toolbar	The Ask toolbar is a browser add-on that is known to hijack the browser, changing the search engine to one provided by Ask and will spawn pop-up messages to prevent users from reverting the changes.	HOST324 HOST047

"SHADOW IT" SOFTWARE

Shadow IT is any application or other IT resource obtained or built by business users without the knowledge or approval of the IT department, and it is becoming a pervasive problem. Business users say they resort to shadow IT to save time and money, but this practice of surreptitiously bypassing the IT professionals creates increased costs for companies. Because shadow applications - also called rogue deployments, rogue IT or stealth IT - are not managed by the IT department or integrated into an organisation's other systems, they are not subject to the same security controls or other compliance-related safeguards. If the IT team is not aware of applications or services procured directly by business users, it may not know where data is stored or who can access it.

Shadow IT did not start with cloud computing or software as a service, but the cloud has made bypassing the IT department easier. It is tough enough to retain control over data that is held within an organisation's own jurisdiction, but the challenge is greatly magnified when data is transmitted, handled or stored by a public cloud provider. It is nearly impossible for IT to manage compliance in the cloud if it doesn't have a well-defined relationship with the service provider.

During the course of the assessment, four Cy1 hosts (HOST31, HOST42, HOST71 and HOST-115) were found to have forensic artefacts that suggest Dropbox, a popular cloud file sharing service, is installed. If use of Dropbox for business purposes is unexpected, CORVID recommends that those four hosts should be the initial focus of an investigation to determine whether Cy1 data has been leaked.

PROCESS ANALYSIS

Typically, for malicious activity to occur, malware must be executed (loaded into main memory) on one or more hosts. In order to detect malware at runtime, PICA analyses every executable file loaded into memory.

Analysis of all process activity across Cy1 resulted in 4,872 out of 27,843,248 process 'creations' being flagged for further automated analysis. The goal being to identify malware and malicious abuse of legitimate applications. This is achieved by inspecting metadata to determine, amongst other things, unusual usage patterns and suspicious process arguments.

During the Compromise Assessment, no evidence of active malware was identified on Cy1's IT infrastructure.

POWERSHELL ANALYSIS

Microsoft PowerShell is a powerful scripting language and shell framework primarily used on Windows computers. It has been around for more than 10 years and will replace the default command prompt on Windows in the future. While many system administrators use PowerShell scripts for daily management tasks, we have seen attackers increasingly using the framework during their campaigns.

Many recent targeted attacks have used PowerShell scripts. For example, the Odinaff group used malicious PowerShell scripts when it attacked financial organisations around the world. Common cybercriminals are leveraging PowerShell as well, such as the authors of the Kotver family of malware, who use the scripting language to achieve a 'file-less' infection, resident entirely within the Windows Registry.

PowerShell is installed by default on most Windows computers, and most organisations do not have extended logging enabled for the framework. These two factors make PowerShell a favoured attack tool. Furthermore, scripts can easily be obfuscated and allow for payloads to be executed directly from memory.

PICA encompasses in-depth analysis of forensic artefacts pertaining to PowerShell activity, including:

- Framework configuration
- Execution history
- PowerShell artefacts within Windows Registry

Whilst no evidence of malicious PowerShell usage was identified, three hosts were identified as having a non-standard (unrestricted) execution policy. This defines those scripts that can be executed by the local instance of PowerShell. By default, this is configured as 'restricted' or 'remote signed'; a policy of 'unrestricted' permits the execution of any script (regardless of source or digital signature).

Though there are legitimate reasons for administrators to modify the policy, we consistently observe threat actors modifying it when interacting with systems during lateral movement. CORVID recommends Cy1 verify the legitimacy of the current Execution Policy enforced on the following hosts:

HOSTS	DESCRIPTION
HOST37 **HOST178** **HOST265**	CORVID recommends Cy1 verify the legitimacy of the Execution Policy currently enforced: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell *ExecutionPolicy REG_SZ Unrestricted*

FILE ANALYSIS

In addition to the analysis of persistent binaries, PICA also performed extensive analysis of other executable files. This facilitates the detection of malware that is resident but dormant (i.e. has not/is not regularly executing). Static analysis of the executable files seeks to identify suspicious binaries in a signature-less fashion, through analysis of:

- Digital signatures (validity and certificate authority)
- Executable structure
- Obfuscated/encrypted payloads
- Suspicious imports (i.e. networking functionality)

In total, PICA performed analysis on 2,182,304 unique files. No evidence of dormant malware was identified on Cy1's IT infrastructure.

EVENT LOG ANALYSIS

Windows event logs are an extremely valuable resource when attempting to detect security incidents. Whilst many organisations collect logs from security devices and critical servers to comply with regulatory requirements, few regularly inspect logs from their windows endpoints; even fewer proactively analyse these logs. Analysing workstation logs is critical because it is increasingly at the workstation level that the initial compromise happens. PICA extracts and processes information from endpoint Event Logs to assist CORVID Analysts with discovering activity of interest. This includes:

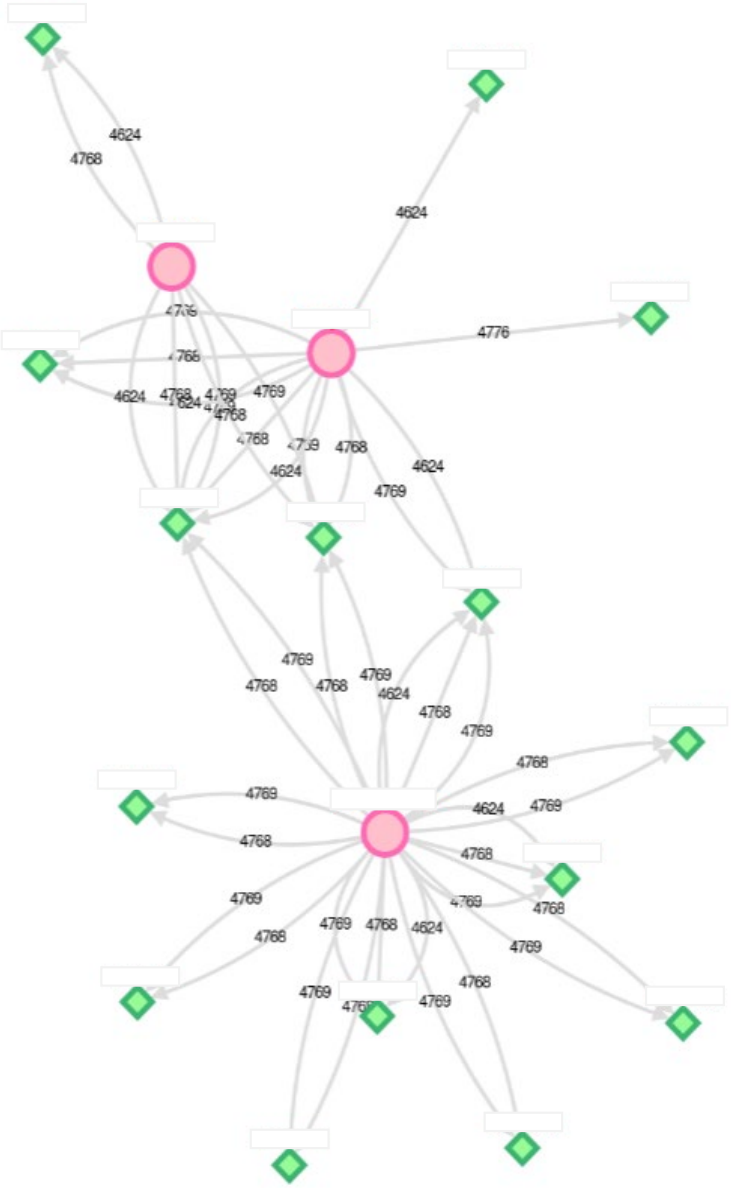
- Application crashes
- System or service failures
- Firewall changes
- Clearing event logs
- Software and service installation
- User account usage
- Protected drivers being altered
- Group policy errors
- External media usage

During the Compromise Assessment, no evidence of suspicious activity was identified on Cy1's IT infrastructure.

LATERAL MOVEMENT ANALYSIS

Throughout the assessment, active and historic network logons were analysed for signs of lateral movement by attackers. Lateral movement refers to the various techniques attackers use to progressively spread through a network as they search for key assets and data. Attackers use lateral movement to pivot between compromised hosts in order to bounce deeper into the network. This process of performing internal reconnaissance and passing malware/tools to successive hosts is often a clear indicator of lateral movement in the network.

As demonstrated by the below graph, although potential lateral movement was detected during the assessment, the activity was investigated and attributed to legitimate network activity by Cy1 IT administrators.



During the Compromise Assessment, no evidence of suspicious lateral movement was identified on Cy1's IT infrastructure.

ADMINISTRATIVE PRIVILEGES ANALYSIS

The weakest link in an organisation's security posture is often the overuse of privileged accounts. Broad privileges are rights and permissions that allow an account to perform specific activities across a large cross-section of the environment. For example, IT administrators may be granted permissions that allow them to reset the passwords on many user accounts.

Deep privileges are powerful privileges that are applied to a narrow segment of the user population. For example, giving an engineer administrator privileges on a server so that they can perform repairs.

Neither broad privilege nor deep privilege is necessarily dangerous, but when many accounts in the domain are permanently granted broad and deep privilege, if only one of the accounts is compromised, it can quickly be used to reconfigure the environment to the attacker's purposes or even to destroy large segments of the infrastructure.

The crux of the problem is two-fold:

1. It is usually trivial for an attacker to obtain deep privilege on a single computer and then propagate that privilege more broadly to other computers.
2. There are usually too many permanent accounts with high levels of privilege across the computing landscape.

Even if credential stealing malware was eliminated, attackers would simply use different tactics, not a different strategy. Rather than planting malware that contains credential theft tooling, they might plant malware that logs keystrokes, or leverage any number of other approaches to capture credentials that have powerful privileges across the environment. Regardless of the tactics, the targets remain the same: accounts with broad and deep privileges.

In Active Directory, it is common to find that the Enterprise Administrators (EA), Domain Administrators (DA) and Built-In Administrators (BA) groups contain excessive numbers of accounts. Most commonly, an organisation's EA group contains the fewest members, DA groups usually contain a multiplier of the number of users in the EA group, and Administrators groups usually contain more members than the populations of the other groups combined. This is often due to a belief that Administrators are somehow 'less privileged' than DAs or EAs. While the rights and permissions granted to each of these groups differ, they should be effectively considered equally powerful groups because a member of one can make himself or herself a member of the other two.

CORVID recommends that Cy1 review the below group members and remove any user accounts that no longer require administrative privileges.

GROUP	MEMBERS	
Domain Admins	Administrator AUser 1 - DA AUser 2 - DA AUser 3 – DA	AUser 4 - DA CR Admin svc backup svc epo
Enterprise Admins	Administrator	SP Admin
Schema Admins	Administrator	AUser 4 - DA

Although endpoints typically have significantly fewer members in their local Administrators groups than member servers do, in many environments, users are granted membership in the local Administrators group on their personal computers. When this occurs, even if User Account Control (UAC) is enabled, those users present an elevated risk to the integrity of their endpoints.

CORVID recommends that Cy1 review the below local administrators and remove any user accounts that no longer require administrative privileges.

USER ACCOUNT	COMPUTERS
acc.name1	ALL HOSTS
acc.name2	HOST-AZURE3
acc.name3	HOST093
acc.name4	HOST243
acc.name5	HOST01, HOST02
acc.name6	HOST-098
acc.name7	HOST02, HOST01, HOST02
acc.name8	HOSTL-036
acc.name9	HOST01
acc.name10	HOST-142, HOST-LS28
acc.name11	HOST01, HOSTX1
acc.name12	HOST-BACKUP11, HOST-XY01, HOST-XY02, HOST-XY03, HOST-E01, HOST-BACKUP03, HOST-LSL, HOST-X7RR
acc.name13	HOST-X8SS
acc.name14	HOST-XY01, HOST-LS28
acc.name15	HOST-X7RR
acc.name16	HOST-026, HOST-074, HOST-086, HOST-101, HOST-126, HOST-131
acc.name17	HOST-036
acc.name18	HOST-HR02

OPERATION CLOUD HOPPER

Security researchers uncovered a pervasive cyberespionage campaign by a group known as 'APT10' (aka MenuPass, POTASSIUM, Stone Panda, Red Apollo, and CVNX). The attacks were levelled against managed IT service providers, which the group used as intermediaries to get their hands on their target's corporate assets and trade secrets.

The campaign has impacted organisations in North America, Europe, South America, Asia, and most recently managed service providers (MSPs) in the United Kingdom, United States, Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa, India, Thailand, South Korea, and Australia.

The MSPs who managed the victims' application, network and system infrastructure were compromised in order to infiltrate the networks of their intended targets: the MSPs' clients. APT10 did not just infect high-value systems. It also installed malware on non-mission-critical machines which it would then use to move laterally into their targeted computers - a subterfuge to prevent rousing suspicion from the organisation's IT/system administrators. APT10 is noted to use open-source malware and hacking tools, which have been customised for their operations, and furtively access the systems via Remote Desktop Protocol (RDP) or use Remote Access Trojans (RATs) to single out which data to steal.

The data is then collated, compressed, and exfiltrated from the MSP's network to the infrastructure controlled by the attackers.

Operation Cloud Hopper highlights the ever-evolving cyberespionage landscape, with the connectivity between MSPs and its customers now being used as an attack vector. For enterprises, it also underscores the significance of carefully assessing and validating the risks entailed when third-party infrastructures are integrated into business processes. MSPs shouldn't simply streamline how their client's system infrastructure is managed; as Operation Cloud Hopper showed, MSPs must also balance its efficiency and the need to secure it.

Apart from keeping systems up-to-date, both MSPs and enterprises should take defensive measures to mitigate these kinds of threats, including having proactive incident response measures.

During the assessment, CORVID security analysts utilised the PICA service to scan Cy1's IT infrastructure for evidence of activity pertaining to APT10 and similar attack campaigns. No evidence of compromise was discovered.

CORAX ASSESSMENT

The CORAX service provides preventative protection against Internet threats as well as detection of extant compromises within an IT infrastructure. It does this by analysing DNS (Domain Name System) name resolution for customers.

DNS is the cornerstone of Internet resource location. Because of DNS, users do not have to remember IP addresses and can use friendlier internet names (domains); such as 'www.corvid.co.uk'.

Attackers use domains for two purposes:

a. To infect computers – users visit a website which is malicious. An attacker will prepare the website to attack the user, taking advantage of a vulnerability resident in the software that the user is reliant upon.
b. To control compromised computers – once a computer is infected, it will be controlled by an attacker. To control the computer the malware establishes communication to a domain that the attacker controls.

CORVID constantly updates the list of 'unsafe' domains within its intelligence database, meaning that customers are prevented from visiting known bad Internet domains. This prevents compromises from occurring in the first-place.

Because it is not possible to know every single domain that is being used maliciously at any point in time, the CORAX service also investigates every domain that customers visit to determine whether or not it could be being used by attackers at that point in time. This intelligence-on-demand feature of CORAX enables CORVID to determine whether certain types of widespread malware is resident within an IT infrastructure.

CORAX is one of three different services used by CORVID to detect a compromised computer within an IT estate. It works purely at the DNS metadata-level; and so is non-invasive (i.e. there is no requirement for specialist software or equipment at the customer site).

One popular technique for malware distribution is through a method referred to as malicious advertising, or malvertising. This technique works when a threat actor buys advertising space on a legitimate web-site; enabling them to execute code against a user even when the user has only visited a "safe" website. CORVID has witnessed campaigns by threat actors that make use of this technique to compromise large numbers of users in a very short space of time.

These campaigns are growing in number and size, and even mainstream websites have inadvertently hosted malicious content to their visitors, such as MSN, BBC, The New York Times, AOL and Newsweek (http://www.bbc.co.uk/news/technology-35821276). Whilst CORAX cannot always prevent this from occurring; it can identify when it occurs and enable an immediate response.

DNS OVERVIEW

This section provides a summary of the internet resources used during the period. This can be an important metric as it shows the amount of interaction between the Cy1 IT systems and the internet during the assessment. Over time, this metric enables resource use and trend analysis to identify:

a. Which internet services the business is reliant upon.
b. Whether internet use is static, growing or diminishing. This information can help decision making regarding the technical resources required to sustain internet service.
c. Typical patterns of Internet use by day/time. This information is used for trend analysis to isolate aberrant behaviour of systems and users.
d. The volume of internet service use compared to other companies within a similar sector.

All businesses make use of the internet, however some customers find comparisons informative regarding whether or not their company is using the internet more, less or the same as similar profiled businesses.

AVG DNS REQUESTS/DAY

428,228 DNS requests

AVG DNS REQUESTS/WEEK

2,997,596 DNS requests

TOP 4 DOMAIN CATEGORIES

- Internet Services
- Entertainment
- Business Services
- Business & News

TOP 10 DOMAINS

The following table represents the top 10 domains (in terms of individual requests) observed during the monitored period.

1	mcafee[.]com
2	akamaiedge[.]net
3	akadns[.]net
4	akamai[.]net
5	edgekey[.]net
6	google[.]com
7	amazonaws[.]com
8	teamviewer[.]com
9	microsoft[.]com
10	cedexis[.]net

AVG OOH DNS REQUESTS/DAY

102,775 DNS requests

On average, 24% of the observed DNS traffic took place out of office hours (OOH), between 21:00 in the evening and 06:00 the following morning (local time).

TOP 5 OOH DOMAINS

1	mcafee[.]com
2	akamaiedge[.]net
3	akadns[.]net
4	akamai[.]net
5	edgekey[.]net

The volume of DNS traffic was higher than expected. However, the volume is not markedly high and could be accounted for because of the extensive use of cloud business services, by the way DNS is accessed/cached locally, or because the period analysed is traditionally busy. On average 24% of the observed traffic took place outside of conventional office hours. As none of the domains visited suggest compromise or non-business focussed activity, the out of hours traffic analysed during the assessment presents no cause for concern.

CONTACT WITH KNOWN BAD DOMAINS

The CORVID Intelligence Database is a continuously updated list of the highest risk domains and IPs on the internet, enabling the protection of customer networks from external threat actors. Traditional blacklists are often prone to false positives and are usually a blind aggregation of other lists. As a result, organisations relying on these lists to protect their business have 'blind spots' that can miss high risk traffic and lead to breaches and compromises. The CORVID Intelligence Database uses sophisticated techniques to ensure our intelligence is relevant and actionable; whilst dramatically reducing false positives.

Part of the CORAX service is to provide just-in-time intelligence, consequently every new domain that is visited by a customer is analysed to determine whether or not it could be being used maliciously when the customer visited it.

During the assessment, CORAX analysed 19,284 unique domains specifically for Cy1. These domains were analysed for high-confidence indictors to determine if they were being used by threat actors at the time of analysis. No activity of interest or advanced malware was discovered to known bad domains during the Assessment.

ADVANCED COMMAND & CONTROL MALWARE

Domain Generation Algorithm (DGA) is a sophisticated method used by malware to 'call-home', or communicate with a Command & Control (C2) server.

DGA generated domains avoid detection by using, what appears to be, random and different DNS names to find a server that it wants to be controlled by.

During the course of the monitored period, whilst 912 domains were analysed by CORAX DGA domain heuristics for signs of DGA activity, no activity of interest was discovered.

BEACON MALWARE

Beacons are frequently employed by malware as a means of signalling successful infection and readiness for instruction for a C2 controller. The beacon connection is often also used as the means of creating a full C2 channel between infected workstation and controller. Typically, beacon traffic exploits the likelihood that the DNS protocol will be able to make contact with arbitrary internet hosts (be that directly or via intermediate servers such as site resolvers or web proxies).

CORVID uses a heuristic behaviour analysis to discover beaconing behaviour based on aspects of the DNS protocol along with time-based analysis. The methods used by CORVID to find beaconing behaviour also highlight non-malicious or less obviously malicious beacons such as those used by the online advertising industry and by software that 'calls home' for updates.

The methods used also highlight non-malicious or less obviously malicious beacons such as those used by the online advertising industry and by the methods used to keep some software packages up-to-date. During the assessment, 1,736 potential beacons were analysed for signs of malicious behaviour, but no activity of interest was discovered.

VARIS ASSESSMENT

Cyber attackers prey on system weaknesses to exploit vulnerabilities in an IT infrastructure, through unpatched software, poorly configured services, default passwords or exposed services.

These vulnerabilities dictate the size of an organisation's attack surface. For many businesses it is not practical to continuously maintain an accurate picture of their attack surface and any potential security flaws leave systems increasingly vulnerable to the wide range of techniques used by attackers.

VARIS works to reduce your vulnerabilities. It scans across an entire IT system to identify vulnerabilities, with the data being examined and interpreted by our analysts. The results are presented in a clear, easy to understand report, prioritising the remediation activity required. The attack surface is tracked over time, giving valuable insight into an organisation's security posture and provides long-term assistance in reducing threat exposure.

Key features:

1. **Identify key vulnerabilities.** Data is interpreted by our security analysts who, after taking account of current attack trends, identify the most pertinent vulnerabilities, and work with IT administrators to manage and mitigate the associated risks.
2. **Reduce attack opportunities.** VARIS scans provide actionable information which can be used to effect change and reduce the opportunities presented to an attacker.
3. **Tracking over time.** VARIS enables the attack surface to be tracked over time, giving valuable insight into the customer's security posture.
4. **Tailored scanning.** CORVID security analysts tailor the scan to meet the specific requirements of each customer, with consideration given to legacy equipment and business critical assets, and scans are designed to be non-disruptive.
5. **Pro-active CORVID management.** Intelligence harvested from CORVID's extensive managed security offerings provide peace of mind that the attack surface is being pro-actively managed.
6. **Evolving database.** The vulnerability database which powers VARIS is constantly evolving as new security flaws are identified.
7. **No additional investment.** VARIS is a managed service, so customers gain the business benefit of improved security without the pain of having to divest time, effort and money in a complex and niche area of technology which is not part of their core business.
8. **Visible security health.** VARIS enables IT administrators to demonstrate an improving picture of security health across their estate. Not only does this provide a real benefit in reducing the likelihood of a compromise, but it illustrates the effort and hard work that is often overlooked in keeping systems secure and up to date.

VULNERABILITY SCAN SUMMARY

The vulnerability scan took place on Wednesday 22 August 2018 and the following asset groupings were in scope:

NETWORK NAME	SCAN DURATION	LIVE ASSETS	HIGH SEVERITY VULNERABILITIES
Cy1 HQ	22h:29m:10s	523	942
Cy1 HQ 2	02h:53m:46s	128	1,892
UK A	00h:36m:48s	16	9
UK B	00h:43m:02s	23	37

KEY FINDINGS

ASSET COUNT	HIGH VULNERABILITYCOUNT	OTHER VULNERABILITIES
		
690*	***2,880***	***1,284***

**A decrease in the expected asset count could be the result of hosts being offline at the time of the scan.*

The scan discovered a total 4,164 vulnerabilities across 690 assets. 2,880 of the discovered vulnerabilities were High Severity. High Severity vulnerabilities usually have most of the following characteristics:

1. Exploitation of the vulnerability likely results in root-level compromise of assets.
2. Exploitation is usually straightforward, in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims, and does not need to persuade a target user, for example via social engineering, into performing any special functions.

For high severity vulnerabilities, it is advised that you patch or upgrade as soon as possible, unless you have other mitigating measures in place.

The below table provides a high level overview of the high severity vulnerabilities extant within Cy1's infrastructure. The table consists of the following columns:

1. **Finding** is the name of the vulnerability grouping. A finding may consist of one or more distinct vulnerabilities grouped together with a common theme. For example, 'Missing Microsoft Hotfixes'.
2. **Recommendation** is the remediation summary.
3. **No. Assets** is the number of assets affected by a given finding.
4. **No. distinct vulnerabilities** is the number of different vulnerabilities in the finding. For example, 'MS15-124: Cumulative Security Update for Internet Explorer (KB3116180)' is a distinct vulnerability within the 'Missing Microsoft Hotfixes' finding.
5. **No. vulnerability instances** is the total number of vulnerability occurrences. Each distinct vulnerability may affect one or more assets.

FINDING	RECOMMENDATION	NO. ASSETS	NO. DISTINCT VULNS.	NO. VULN. INSTANCES
Missing Microsoft Hotfixes and Microsoft Application Vulnerabilities	Test and install the relevant Microsoft hotfixes. Check why some hosts are not automatically receiving necessary hotfixes.	72	178	893
Firefox Web Browser Critical Vulnerabilities	Upgrade to the latest version of Firefox.	23	38	528
Adobe Flash Player Vulnerabilities	Uninstall Adobe Flash Player. If there is a business requirement for Flash Player then upgrade to the latest version.	24	39	512
Adobe Reader and Acrobat Vulnerabilities	Upgrade to the latest version of Adobe Reader.	29	10	278
Java Vulnerabilities	Upgrade to the latest version of Oracle Java.	19	24	191
Google Chrome Web Browser Vulnerabilities	Upgrade to the latest version of Chrome.	4	3	27
VMWare Vulnerabilities	Apply relevant patches or upgrade to the latest version of VMWare.	5	2	24
Wireshark Vulnerabilities	Apply relevant patches or upgrade to the latest version of Wireshark.	3	8	13
TLS/SSL Weaknesses	(see individual recommendations contained in the full vulnerability report)	36	3	38
Other	(see individual recommendations contained in the full vulnerability report)	59	34	128