The Evolving Cyber Threat to the Banking Community

Executive Summary

There has been a significant evolution in the cyber threat facing the global financial industry over the last 18 months as adversaries have advanced their knowledge. They have deployed increasingly sophisticated means of circumventing individual controls within users' local environments, and probed further into their systems to execute well-planned and finely orchestrated attacks.

The groups behind these attacks are deploying ever more creative techniques to access users' critical assets. These include gaining Administrator rights for operating systems, manipulating software in memory, and tampering with legitimate functionality to bypass two-factor authentication. Highly covert malware is now being deployed, designed to withstand traditional detection techniques. Furthermore, in any single attack a mix of malicious files will often be used, whether that be to acquire credentials or to bypass authentication requirements; to learn how internal operations or messages work; to create distractions and delay local security teams' responses; or to securely delete log files and other traces of the attacks. Forensic investigations are increasingly being hampered by the attackers' efforts to erase their activity and obscure their techniques.

It is clear that the adversaries are prepared to invest considerable time in planning and preparing for attacks. In some cases we have been able to observe that the attackers had been quietly present on customers' systems for longer than 12 months before actually attempting to execute the frauds – often doing so around public holidays.

The determination, patience and cunning the attackers are demonstrating makes it more imperative than ever that customers rapidly deploy and maintain all basic cyber hygiene tools and measures, comprehensively adhere to recommended security controls, and incorporate all the elements set out in SWIFT's Customer Security Programme.

There is no single solution, silver bullet or one-time implementation that will protect against this complex threat-stream. Similarly, just as it must be understood that cybersecurity is a continuous process rather than a static end state, no system can be assumed to be totally infallible, or immune to attack. That said, there are ways in which users can best protect themselves from the complex methods deployed against them – and they must be used. In all the cases we have seen, the attackers have been able to exploit basic security weaknesses in users' perimeter and internal network security. Security must be built into the DNA of networks, organisations and employee mind-sets. Defence must be built "in depth" through the combination of multiple layered components, barriers and counter-measures. Relying on any single defence or component, or even a subset of components, is no defence at all.

The rise in the threat level clearly requires a concerted response. While each individual customer has to be responsible for its own security, SWIFT is committed to continue playing an important role in reinforcing and safeguarding the security of the wider ecosystem. The security of the community requires *everyone's* participation – starting with each individual participant's own organisational security.

The security of the community requires everyone's participation – starting with each individual participant's own organisational security.

Background

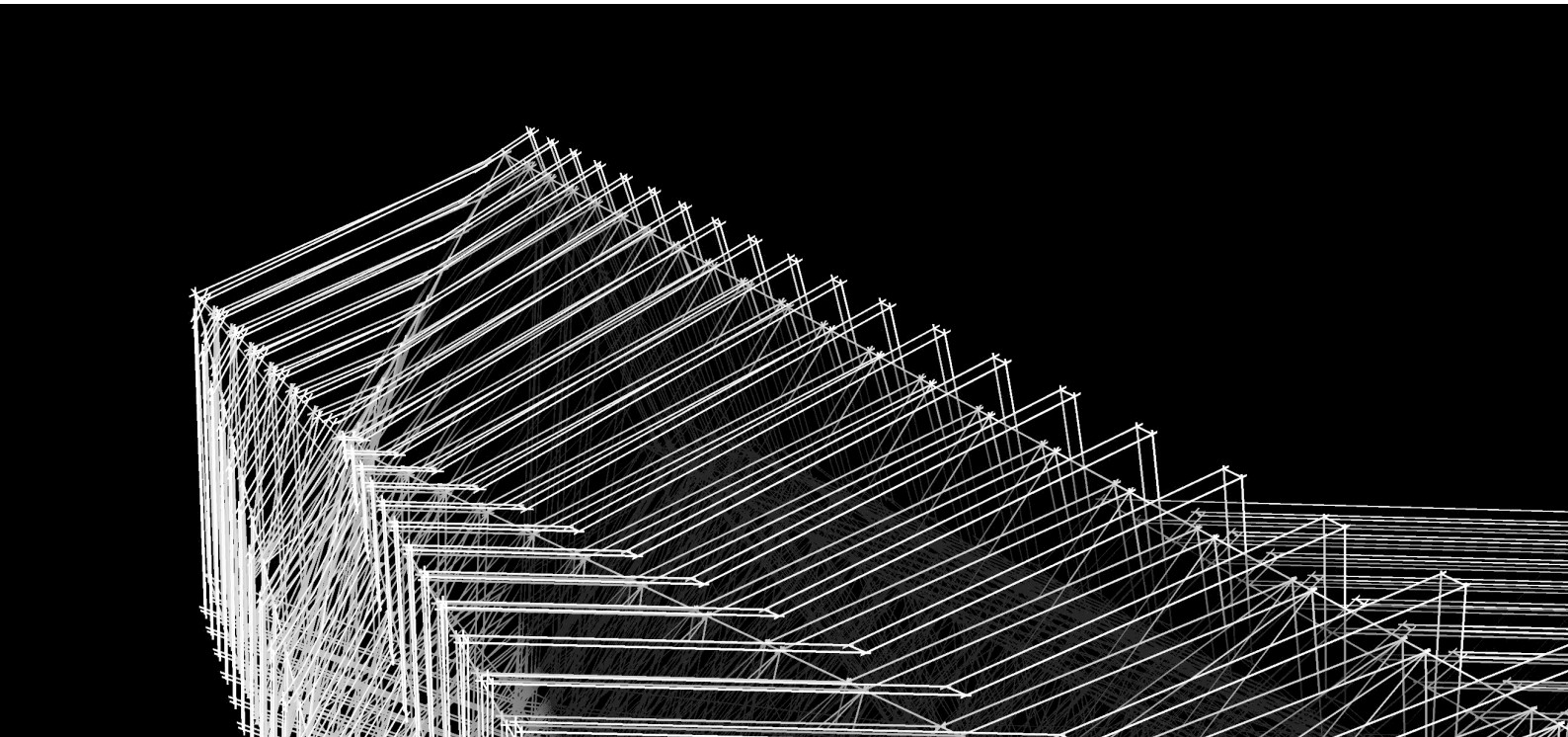
The February 2016 attack was a watershed moment for the payments industry. Though not the first case of fraud against a bank's payment endpoint, it was the scale and sophistication of the attack which shook the global community.

The perpetrators not only had a detailed knowledge of the business processes involved in interbank payment messaging, but also reverse-engineered the specific interface software running in the victim bank. With this knowledge they built custom malware both to aid sending fraudulent messages and to cover-up the evidence to enable their getaway. This was all co-ordinated with the precision of a military operation, taking advantage of a local public holiday to further hamper the victim's response.

The attack also opened a 'Pandora's Box' as further cases came to light and criminal groups ramped up copy-cat attacks. Software updates were released to mitigate specific attack vectors – such as improved integrity checks to hamper the attackers' ability to modify the software and database. However, the attackers continued their reverse-engineering efforts and updated their malware too. This became a game of cat-and-mouse through successive attacks.

In all cases, security weaknesses in the compromised banks led to the attackers' gaining Administrator access to their payment environments. With this they could not only monitor the victim banks' operations undetected over extended periods, but they could also modify victims' security defences and the operation of their software to enable their attacks – updating firewall rules, and bypassing security features in the interface software.

Since then, the attacks have continued to evolve. On the following page is a specific example, followed by brief explanations of some of the techniques being used.



Case Study

A customer suffered an intrusion into their internal payments systems, followed by an attempted transfer of US dollars to overseas beneficiaries.

Compromise the Customer's Environment

The initial intrusion vector is unknown. However, once the attackers gained access to the customer's environment, they acquired administrator credentials and with these they updated Windows firewall rules to allow them to deploy covert malware which would allow them to remotely control the victim's systems. The malware resides only in the memory of machines it is deployed on – leaving little footprint on the infected systems for traditional security tools to detect.

This malware is designed to passively 'listen' for incoming commands relayed across a network of 'hops', including relays within the bank's network itself. This allowed the attackers to execute a large set of different actions on the target system remotely.

Obtain Valid Operator Credentials

The attackers deployed key-loggers and screenshot grabbers to perform reconnaissance and monitor their target. These could be synced and replayed to the remote attackers to provide rich insights into how the customer's staff use and administer their applications and systems.

The attackers carried out this reconnaissance phase for several months on the victim's network, observing and waiting patiently until the opportune moment.

Submit Fraudulent Messages

The final phase of the attack came on the day before a local public holiday.

In the middle of the night local time, the attackers deployed additional malware tools. These had been custom-designed to subvert the version of messaging interface software being run by the customer. Specifically, the malware was designed to modify elements of the sign-on functionality on the messaging interface – bypassing the multi-factor authentication.

With the authentication control subverted, the attackers then copied pre-formatted messages into the customer's messaging interface and distributed payment messages to banks in multiple countries. After several months in the customer's environment the attackers only took three hours to complete this phase of their attack.

Hide the Evidence

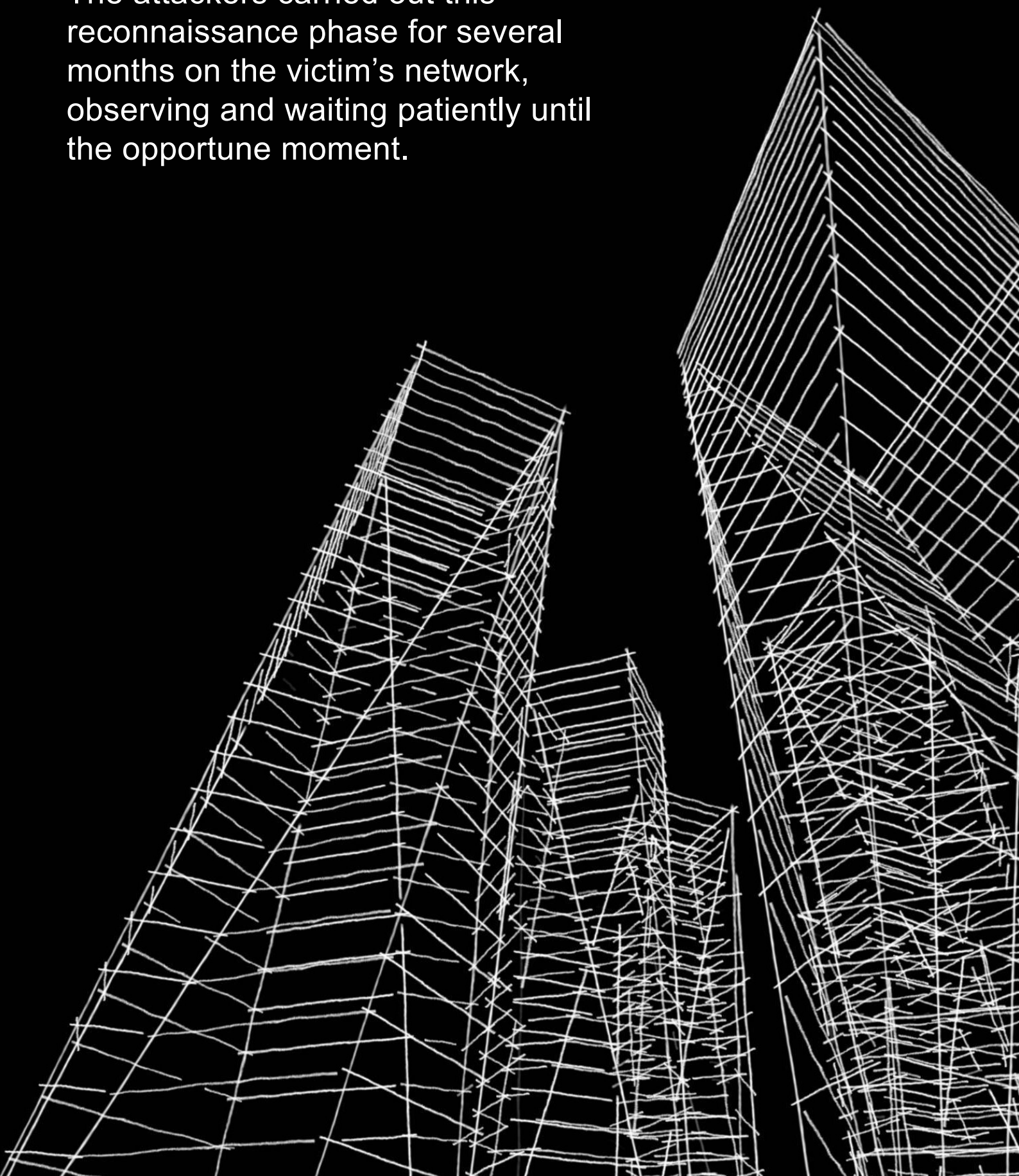
The attackers then set about disrupting the response to the attack and removing evidence of their actions. They used another custom tool to securely overwrite files such as Windows Event logs and Prefetch files – which contain key information that forensic investigators rely on for evidence.

As their final act they deployed ransomware which spread across the victim's network (using the previously obtained administrator credentials) and locked documents with an encryption key.

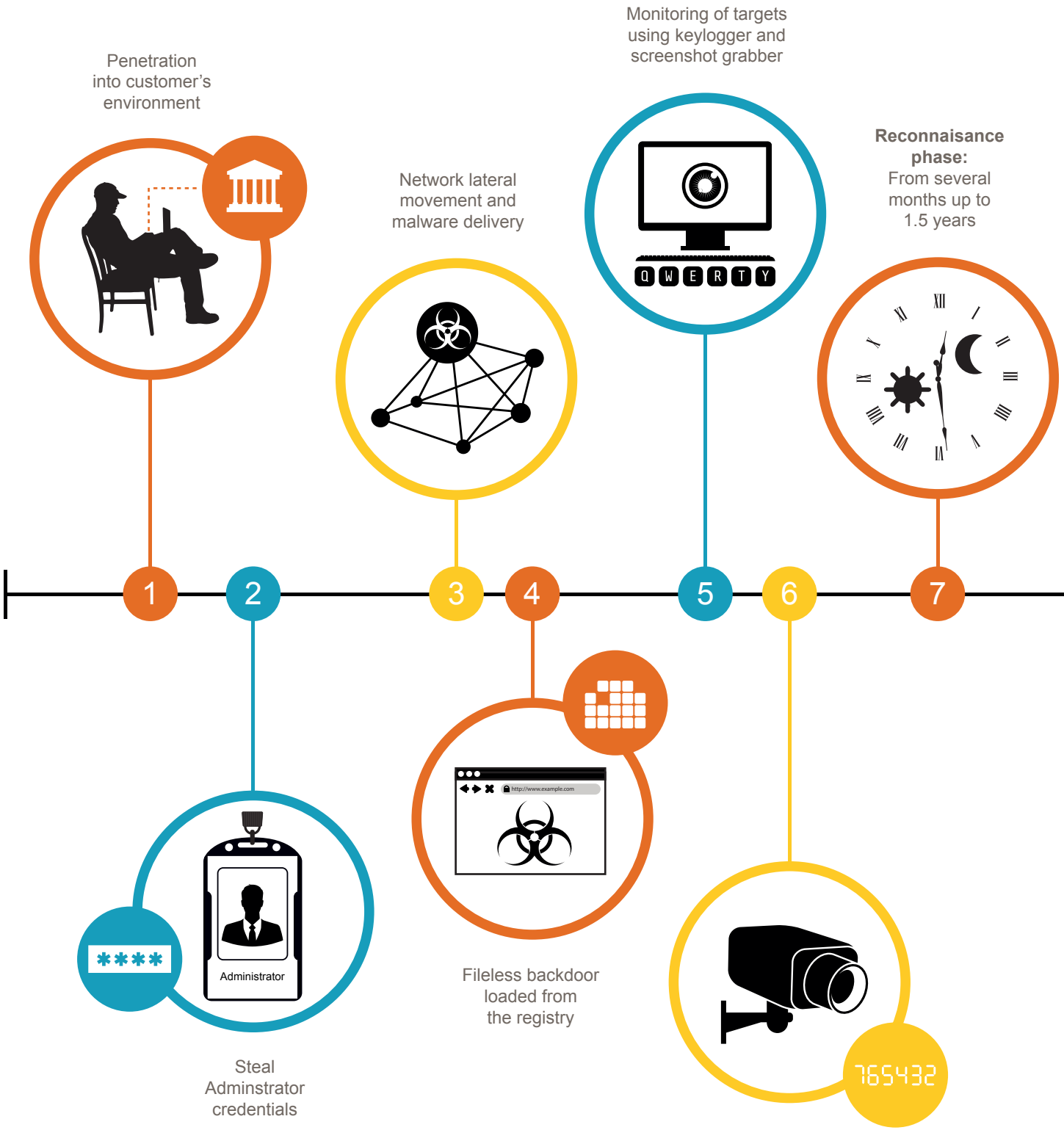
Dozens of the customer's machines were infected with this, creating a major incident for its IT security team as they arrived into work in the morning. This malware, though fully functional as ransomware, was likely a smokescreen for the real attack targeting the customer's payment systems.

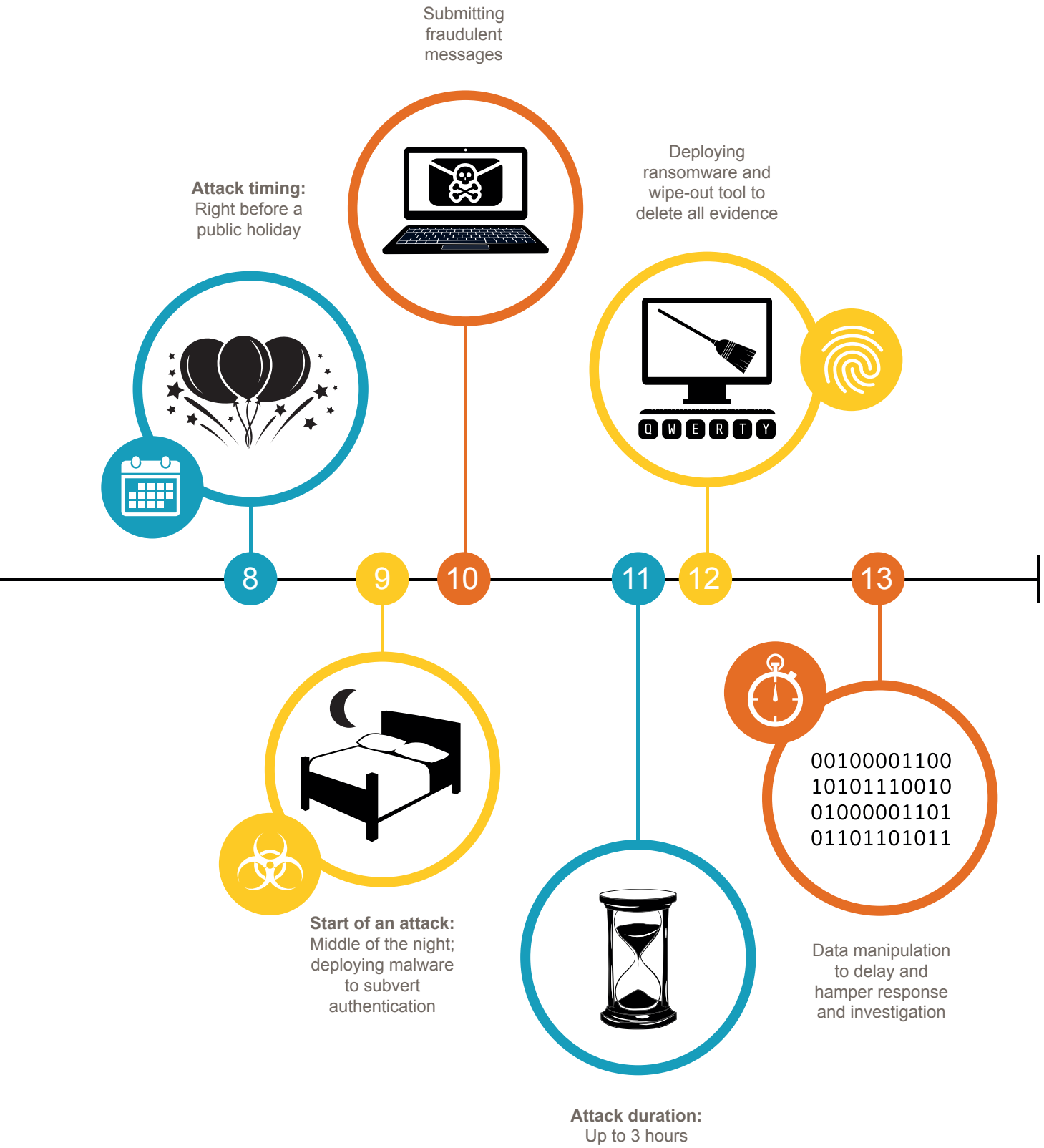
Fortunately, the customer quickly identified the fraudulent payment messages and contacted authorities overseas who moved quickly to freeze the stolen funds.

The attackers carried out this reconnaissance phase for several months on the victim’s network, observing and waiting patiently until the opportune moment.



Chronology of an Attack




Submitting fraudulent messages
Attack timing: Right before a public holiday
Deploying ransomware and wipe-out tool to delete all evidence
QWERTY
8
9
10
11
12
13
00100001100
10101110010
01000001101
01101101011
Start of an attack: Middle of the night; deploying malware to subvert authentication
Attack duration: Up to 3 hours
Data manipulation to delay and hamper response and investigation

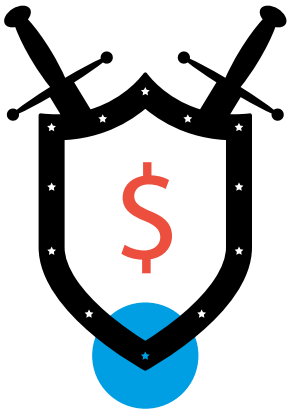
Evolving Attack Techniques

Deep analysis of different cases reveals that the attackers are using existing best-of-breed techniques, leveraging legitimate and malicious functionality. The use of these techniques has been mastered through successive attacks, leading to the sophisticated toolkits we have observed in recent months. We expect this sophistication to continue to rise. The attackers utilise a number of techniques, some of which are described here:

Protection

For years, the developers of legitimate commercial closed-source software were challenged with the task of hiding intellectual property contained in the software that they build. To prevent their software from being analysed and their secrets revealed, they sometimes rely on commercial software protectors.

Cyber attackers have a similar problem and want to protect their malware, so also chose the very same commercial protection software, such as Enigma or VMProtect – protection that is notoriously difficult to break.



Stealthiness

Attackers want to operate in their targets' environments without being detected, and therefore need to be stealthy in their operations. Malware seen in recent cases used fileless modules that were loaded into memory from the registry. When files are written to the hard drive, they are encrypted and camouflaged in order to blend with other legitimate system files. As a result, the Administrators of systems were unable to distinguish the malicious components from the parts of the operating system.

Wipe-Out Techniques

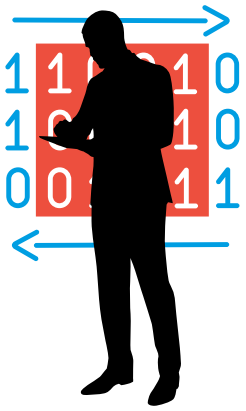
The attackers employ a number of effective anti-forensic techniques to reliably erase all traces of their own activity making retracing and understanding their actions difficult.

In other words, the attackers hope that when the investigators examine a cybercrime scene, they will not find any digital fingerprints.

Hijacking

The attackers have attempted to hijack legitimate software in order to manipulate its logic. One malicious module recovered from a crime scene was programmed to always return “success” result, even if the software attempted to throw an alert.

Hijacking system calls allows the attackers to monitor data in transit. On top of that, intercepted data can also be changed, so that the end parties receive modified information without even knowing that the data was changed.



Surveillance

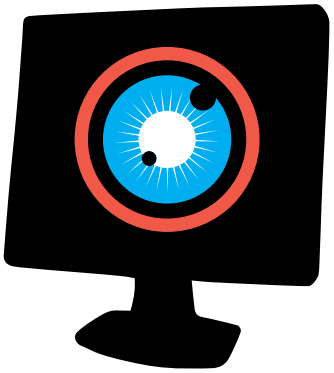
The attackers have deployed malicious modules that took screen shots (frames) along with the typed keystrokes. The intercepted frames were encoded in a way that resembles a video format, potentially allowing them to be reassembled into viewable recordings.

The reconstructed surveillance videos could then have been watched by a group of attackers, with an ability to stop, rewind, take notes, questioning every step taken by an administrator in order to fully understand how the system works before an attempt is made to subvert it.

Fully understanding the legitimate business process is not a quick task, in some cases the attackers spent more than a year studying the process.

The attackers do make mistakes however; in a recent case they left this recording running whilst they interacted with the system, capturing their own activity.

This is analogous to bank robbers setting up an advanced surveillance system to monitor the banking employees’ actions, only to later then also record themselves robbing the bank.



False Flags

In an attempt to put investigators off the tracks, the malware authors placed false flags within their tools, incorporating fictitious tell-tale signs into the code.

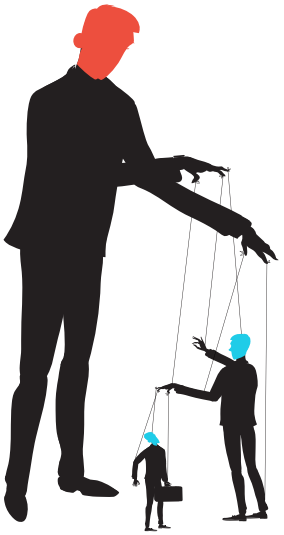
Among these ‘false flags’ are diversionary language codes and various incorrectly transliterated words to mislead research into the true identity of the attackers.

Anonymity

In order to hide their tracks, the attackers set up a number of the ‘hops’ or proxies between themselves and the end-target, making a long chain for investigators to trace in order to understand what is going on.

This is similar in concept to controlling a puppet via another puppet. At any given moment, this keeps the attackers out of direct line of sight.

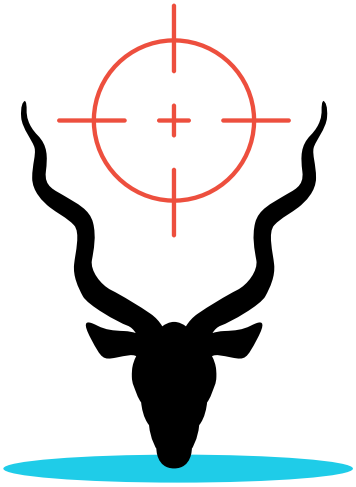
If the number of such “puppets” is large, such as more than three, it may be very difficult to establish who the real mastermind behind the attack is.



Watering Holes

In order to target the victims, the attackers do not engage them directly.

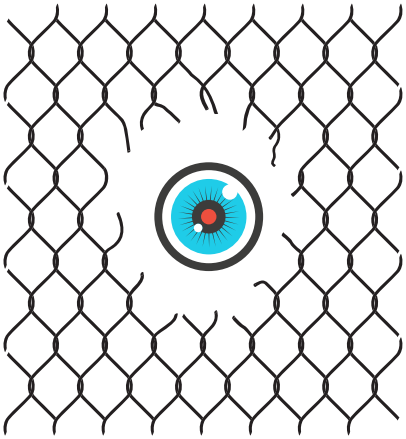
Instead, they ‘bait’ a legitimate web site first. Next, they wait patiently for the victim to come and visit that web site. If the visitor is of interest, say a bank employee, then they attempt to infect the machine of that victim.



Exploits

The attackers are constantly searching for ‘holes’ in the system. Once they find a hole, they penetrate the system, compromising its nodes one after another.

This creates an asymmetric defender-attacker paradox, where the attacker only needs to find one hole to get in, but the defender needs to fix all holes to be secure.



Basic Defences, Counter-Measures and Best Practices

Failure to secure your systems and networks leaves you exposed to attacks such as these. No system is totally bulletproof, but there are ways in which customers can best protect themselves from the complex methods deployed against them – including by preparing for attacks actually succeeding.

Defence in depth, wherein strength is derived from the combination of multiple, layered components, is essential to combatting the threats the community is up against. Customers need to deploy multiple layers of defence. This means ensuring both logical and physical security; protecting and monitoring both external and internal network layers. It entails constant monitoring – as well as the ability to rapidly respond to any alerts; it involves ensuring that there are additional defences around critical systems, and detection measures in place around and within them to identify potential intruders.

At all these layers, host machines must be hardened; strict password, privileges and permissions policies must be in place (and protected) and system and anti-virus software must be updated and upgraded. In addition to all this, security policies must be devised, applied and routinely reviewed to ensure their continued relevance. Finally, personnel must be trained, kept aware and incentivised to prioritise security.

As part of a multi-layered defence to assist in safeguarding your local environments and reinforcing the security of the global financial community, customers should:

Secure your Environment

Embedding security in the design of your network architecture should be a core principle of your approach. This should include physical security measures, such as limiting access rights to sensitive areas to authorised personnel, and ensuring you have processes in place to actively control and monitor who is accessing these areas. In addition, those authorised personnel must be properly screened and trained.

You should ensure you have robust and clearly defined perimeter security, with appropriate prevention measures, such as firewalls and filters, and detection capabilities in case of intrusion. Through the construction of multiple barriers you should defend from the inside by segregating internal networks according to business needs and risk requirements and you should actively monitor internal networks and harden host machines. On your most critical systems, which should be isolated from the internet, you should deploy a further layer of defences and detection measures. As a matter of course, you should install the latest versions of anti-virus and system software, and immediately implement the latest security updates.

Know and Limit Access

After constructing these defences to guard against intruders coming through the front door, you must put in place operating procedures and processes to limit and protect administrator and system privileges. Having locked down these privileges, a rigorous implementation of strong ID management is required with strict and actively managed profile and password rules to ensure basic access controls.

Further limits should be instigated to control access such as the consistent use of two-factor authentication across all sensitive or critical applications to harden access and provide another layer of defence. In addition you must identify and protect access rights to all your critical systems, such as your interfaces to SWIFT and other payment gateways. These access rules should clearly allocate rights and capabilities to separate roles and ensure that no single operator can – intentionally or otherwise – open systems to potential abuse.

Detect and Respond

Preventative measures will only go so far; detection and response are equally critical. Vital to your awareness and ability to respond in a timely fashion, is having adequate intrusion detection capabilities, delivered through a series of triggers and trip-wires to initiate alerts to suspicious activity. You should actively monitor networks and systems activity, including by monitoring interfaces to SWIFT and other payment gateways for unusual behaviour, such as users logging in at random times of day, users logging in from new or unknown systems or multiple failed password attempts.

Overall, security policies must be devised, applied consistently and regularly reviewed to ensure their continued relevance – and authorised personnel must be trained, kept aware and incentivised to prioritise security. Where you identify gaps in your capabilities or layers of defence you may decide to employ carefully selected cyber security professionals to ensure your local environment is sanitised and properly defended with the latest anti-virus applications.

Complementing and reinforcing these basic security measures, is a range of tools and processes that you should deploy and implement:

Threat Intelligence

Knowing your adversary is vital to protecting against it. Threat intelligence plays a key part in assisting software development and updates to anti-virus applications, and a vital reason why sharing information on known attacks is so important to the whole financial ecosystem. You should also routinely digest such information, including the security bulletins published in the SWIFT Information Sharing & Analysis Centre (SWIFT ISAC); scan against the Indicators of Compromise we provide; and implement the recommendations to ensure you are up to date and your armoury is strengthened against emerging threats.

Limit Exposures

You should only do business with trusted counterparties – and only maintain relationships with those that you trust. SWIFT's Relationship Management Application (RMA) supports customers by enabling them to control counterparty relationships through RMA tools. Regular RMA maintenance – including monitoring any changes to RMA relationships and removing any non-current relationships – is another key way in which you can limit your exposure to potential threats.

Security Controls

Engaging in regular security benchmarking and security audit exercises enables you to detect gaps and lapses in your security controls. To help you in this, SWIFT, in conjunction with industry experts, has published a set of security controls based on the latest cyber-threat intelligence. These controls reflect good security practice and should also apply beyond the SWIFT-related infrastructure into the broader end-to-end transaction chain. All users must implement these controls on their local SWIFT-related infrastructure and self-attest against them, not only to assure yourself you have acted comprehensively to protect yourselves, but to also demonstrate to other users that you have taken all precautions and do not present a risk to others.

Know Your Counterparts

Your understanding of potential counterparts' credit and compliance risks is key to your decision-making around whether and how you do business with them. Cyber considerations should also form an integral part of these routine KYC processes. From January 2018 you will be able to assess who you are doing business with by requesting their self-attestations against the security controls, and to re-assure yourself that your counterparts are taking the necessary precautions and protections, so they do not present an unacceptable risk to you. If you have concerns, you can then act to put in place relevant controls calibrated to the perceived cyber-risk presented by senders.

Other Business Controls

By deploying further business controls you can take timely pre-emptive and corrective action against suspicious activity. For instance, by filtering outgoing messages against a tightly configured set of rules you can screen your outgoing payments to detect illicit or unusual message flows. Being able to detect such out-of-policy messages before they are sent may alert you to a potential compromise, allow you to take immediate remedial action, and ultimately prevent fraudulent transfer requests even leaving your organisation.

As a further precaution you should check on messaging activity ex post. In the first instance, ensuring that your organisation checks its confirmation and statement messages to verify that these accurately reflect approved activity is a simple routine which can help alert you to potential fraudulent messages that have been sent, allowing you to rapidly take corrective actions. Additionally you can undertake secondary checks against independent sources of outbound network activity, to give you an additional layer of quality assurance. To help you in this, SWIFT's Daily Validation Reports offer both a secondary check on transactions to help prevent and detect fraud; and a focused review of large or unusual flows.

Incident Response

Security is not an absolute state – preparing for the worst is as important as defending against it. You must develop and institute a recovery policy to ensure you are equipped to quickly respond to fraudulent activity. If fraudulent or suspicious activities are detected, appropriate actions need to be taken immediately. With the right processes in place, customers may have an opportunity to minimise fraud loss or increase the likelihood that funds can be recovered.

When a customer suspects a fraudulent message has been sent, they need to send a cancellation message – so knowing how to do so is critical. It is vital to know, for instance, that cancellation messages should be flagged to indicate to the recipients that the cancellation is associated with fraud and should be prioritised and pushed to the top of the processing queue so that appropriate action can be taken to hold or freeze funds.

Equally important is ensuring that you have an understanding of the internal actions you must take when responding to an incident – as well as rehearsed processes to support these.

Customer Security Programme Principles

It's important to remind yourself of the principles of SWIFT's Customer Security Programme.

You: Secure and Protect

Securing your local SWIFT-related infrastructure and putting in place the right people, policies and practices, are critical to avoiding cyber related fraud.

To support the industry, SWIFT has published a core set of mandatory security controls and an associated assurance framework for its users. The security controls build upon SWIFT's existing security guidance, taking into account the latest intelligence on known cyber threats and incidents.

Your Counterparts: Prevent and Detect

Companies do not operate in a vacuum and all SWIFT users are part of a broader ecosystem. Even with strong security measures in place, attackers are very sophisticated and you need to assume that you or your counterparts may be the target of cyber-attacks. That's why it is also vital to manage security risk in your interactions and relationships with counterparties.

Strong detection measures need to be put in place to increase the chances of stopping or mitigating fraud in case your environment is breached.

Your Community: Share and Prepare

The financial industry is truly global, and so are the cyber challenges it faces. What happens to one company in one location can easily be replicated elsewhere in the world.

If you been targeted or breached, it is vital that you share all relevant information and let us know there is a problem as soon as possible. SWIFT will then share anonymised information on Indicators of Compromise (IOCs) across the community to help limit further impacts.

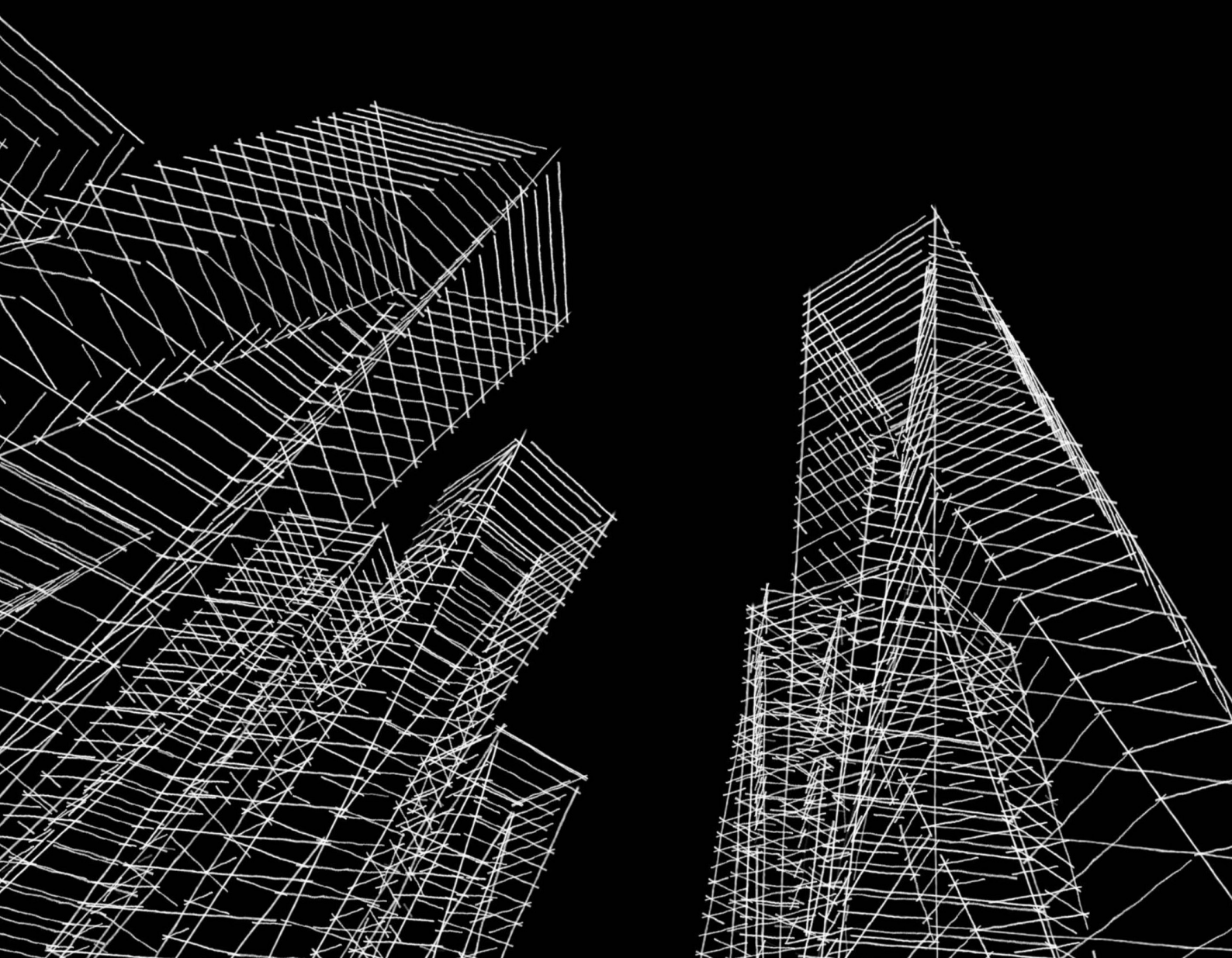
SWIFT will inform you of relevant cyber intelligence, and continues to expand our information sharing platforms to do so. But we also expect you to prepare by acting in a timely manner on the information and security updates we provide, and by ensuring that you meet mandatory security controls for your SWIFT-related infrastructure.

A Common Threat.
A Shared Commitment.

Evidence from recent cases clearly demonstrates the attackers' adaptability, patience, determination and growing sophistication. The rise in the threat level requires an equally concerted response. While each individual customer has to be responsible for its own security, a community-based approach is the best way to solve the security issues facing the industry. This is why the Customer Security Programme has been developed and will continue to evolve in close collaboration with the SWIFT community.

SWIFT is committed to continue playing an important role in reinforcing and safeguarding the security of the wider ecosystem. Through the Customer Security Programme we are devising innovative ways of countering the threat and we are actively investigating cases and potential threats; every time we identify an emerging attack pattern or technique, we publish detailed security bulletins in the SWIFT ISAC, informing customers of any related indicators. Alongside this, we aim to provide our customers with the tools they need to help protect their local environments and ensure that our ongoing security updates assist in countering the very latest tactics. Updates to our software contain critical additional measures to counter the latest evolving threats and build in greater resilience, providing greater protection and security.

The security of the community requires everyone's participation – starting with each individual participant's own security.



About SWIFT

SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services.

Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way. SWIFT's Customer Security Programme, which launched in June 2016, is a dedicated initiative designed to reinforce and evolve the security of global banking, consolidating and building upon existing SWIFT and industry efforts. Within the Programme, SWIFT has established an information sharing initiative and created a dedicated Customer Security Intelligence team, bringing together a strong group of IT and cyber experts.

The team undertakes forensic investigations on security incidents within customer premises related to SWIFT products and services; the related intelligence is published in a readily readable and searchable format in the 'SWIFT Information Sharing and Analysis Centre' (SWIFT ISAC) a global portal which is available to the SWIFT community. By feeding back this intelligence in anonymised form to the wider community, SWIFT aims to help prevent future frauds in customer environments.

About BAE Systems

BAE Systems help nations, governments and businesses around the world defend themselves against cyber crime, reduce their risk in the connected world, comply with regulation, and transform their operations.

We do this using our unique set of solutions, systems, experience and processes - often collecting and analysing huge volumes of data. These, combined with our cyber special forces - some of the most skilled people in the world, enable us to defend against cyber attacks, fraud and financial crime, enable intelligence-led policing and solve complex data problems.

We employ over 4,000 people across 18 countries in the Americas, APAC, UK and EMEA.

SWIFT, Avenue Adèle 1,
B-1310 La Hulpe, Belgium

W: swift.com

linkedin.com/company/swift

twitter.com/swiftcommunity

BAE Systems, Surrey Research Park, Guildford
Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/swift

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai