

THE VISION

EXPERTISE DELIVERED STRAIGHT FROM THE FRONTLINES OF CYBER ATTACKS

FIREEYE TOPS FORRESTERS REPORT



Page 3. FireEye leads the field with its collective capabilities.

GET ONE STEP AHEAD OF EMAIL ATTACKS



Page 4. We look at how email is every organization's most vulnerable attack vector.

NORTH KOREA'S UN-USUAL SUSPECTS



Page 6. The Vision looks into the operations of APT38.

FIREEYE GLOBAL WEBINAR SERIES



Page 8. An excellent resource for cyber security professionals.



Facing forward Cyber security in 2019 and beyond

FireEye's security predictions report – Facing Forward: Cyber Security in 2019 and Beyond – combines the top-down views of some of our senior leaders with an in-depth look at emerging threats from specialized analysts and researchers from FireEye Threat Intelligence, FireEye Mandiant and FireEye Labs.

Our CEO Kevin Mandia, CSO Steve Booth, intelligence authority Sandra Joyce, cloud guru Martin Holste and aviation expert Christopher Porter take a view from the top on subjects as diverse (yet synergistic) as nation states' offensive capabilities, the vulnerabilities of the cloud, the widening skills gap and the continuing threat from ever more devious executions of social engineering.

A vastly increasing number of enterprises are moving their data to the cloud, and whether your view is that it is more or less secure, this is where the attackers are going too. This makes it imperative that you ask the right questions of not only your cloud vendors, but inwardly, of your organization, its business model, infrastructure, resources, employee behaviors and your own hunches.

Hostile activity by nation states is on the increase, not only in volume but in the diversity of emerging actors and their diverse motives. For example, the Chinese Belt and Road development strategy involving infrastructure development and investments in Europe, Asia and Africa is anticipated to drive new cyber threat activity. Regime-sponsored or endorsed activity originating in Iran uses social media to influence audiences around the world on the country's politics. And the North Korean regime is increasingly leveraging the country's cyber criminal capability as international sanctions hit harder. In the meantime, Russia continues to extend its activities with a number of motives.

Aviation is also covered in the report as a particular sector which faces varied, multilateral threats. There has long been speculation around whether it is possible to hack an aircraft. The Department of Homeland Security claims that technically, it is possible. In reality, however, it's unlikely. The more realistic cyber threats to the sector – which are actually happening today – include espionage committed against manufacturers of both military and civil aircraft and their components, data and financial theft from operators and ticket sellers, and ransomware attacks against airports with the objective of either disruption or financial extortion.

In cases such as the latter, it should not be considered unreasonable for passengers to get 'spooked' by such high-profile hostile activity, in turn impacting revenues and reputation.

In addition to the above and other trending threats, the report describes how the tactics, techniques and procedures traditionally used by APT groups and other organized cyber crime gangs are still reaping success for their perpetrators as levels of sophistication are added in order to evade detection and prevention:

Email is still the most prevalent initial attack vector, representing the point of entry for 91% of attacks. Here, we have observed an increase in the use of password-protected malicious attachments to feign authenticity, and CEO and business email compromise fraud activity. SIM card spoofing – effectively bypassing 2FA – is also on the rise. Financial and espionage actors alike are making increased use of open-source malware as well as exploiting legitimate internet services for command and control (C2) purposes.

[Read the full report here >](#)



“The thing to keep in mind is that any foothold that any adversary gets into a system that’s used for cyber espionage, which is widespread and everyone does it, that can easily be turned into an attack.”

Christopher Porter

FireEye helps DHS understand threats to US aviation sector

On September 6th 2018, FireEye Chief Intelligence Strategist Christopher Porter gave expert evidence to a joint hearing by the Cybersecurity & Infrastructure Protection and Transportation & Protective Security Subcommittees on the Homeland Security Committee, in Washington DC.

The hearing set out to examine the current cybersecurity threats facing the aviation sector, and explore ways in which the industry is looking at cyber security in general. The objective was for Congress to find ways that the Department of Homeland Security can provide better assistance in bolstering the overall cyber security of the aviation ecosystem. Porter was joined by Jeffrey Troy, Executive Director, Aviation Information Sharing & Analysis Center and Michael Stephens, Executive VP, IT and General Counsel, Tampa International Airport.

Porter introduced FireEye by explaining that the company supports the aviation sector in the US by protecting the Transportation Security Administration with both email and web inspection, managed by the DHS Enterprise Security Operations Center. The FAA also utilizes FireEye’s intelligence reporting and also uses its malware analysis tool to help prevent and detect future cyber attacks.

“The thing to keep in mind is that any foothold that any adversary gets into a system that’s used for cyber espionage, which is widespread and everyone does it, that can easily be turned into an attack.” Christopher Porter

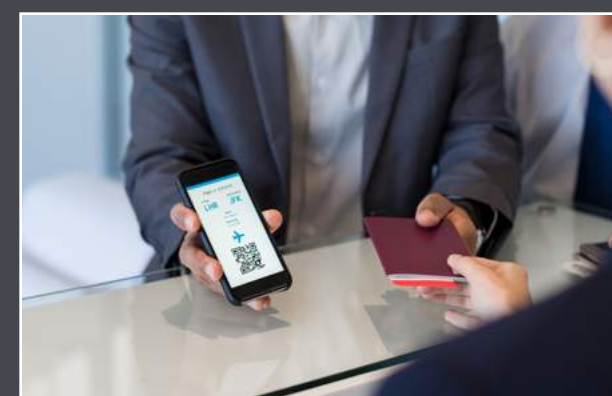
He went on to share FireEye’s perspective responding to breaches in the aviation sector and, from intelligence collected, on anticipated forthcoming threats in this, one of the most targeted sectors for cyberattacks. The main areas of concern – based on intelligence on actual activity by hostile actors – were cited:

1. Cyberespionage

Nation-sponsored or endorsed actors – including those from China, Russia, and more recently Iran – routinely seek to steal industrial secrets from manufacturers, researchers, designers, and operators of both military and cutting-edge civilian aircraft by targeting the US or its close allies via network operations.



All three countries also routinely target ticketing and traveller data, shipping schedules and manifests – as well as partner industries such as railways and accommodation providers – as they gather counterintelligence data on travellers who could be from the worlds of industry, government, media or other VIPs of interest.



2. Economic threats

Porter highlighted three principal ongoing threats to economic wellbeing: For years, airlines and third-party ticket sellers have been compromised to facilitate the re-sale of illicit tickets for profit in underground forums. Exploiting the trust placed in them by their customers, airlines are frequently the targets of theft of a wide variety of sensitive personal data. FireEye devices have detected a sharp increase in the use of ransomware to temporarily disable ticketing and support operations, with cyber criminals cognizant that carriers and airports will avoid disruption.

3. Hacktivism

Airports in the US, Europe, the Middle East and South East Asia have had their websites defaced or disrupted, principally by non-state actors seeking to draw attention to a particular political, social or moral cause. This can lead to passengers fearing that they or a loved one may be at risk of a terrorist attack or hijacking, whereas in reality, the compromised systems have no relationship with flight operations... unless such disruptive activity is perpetrated by cyber criminals who have affiliations with terrorist groups.



In a limited number of cases, such hacks have caused flight delays and other damaging disruption, impacting both revenues and reputation. Porter emphasised that FireEye looks forward to working alongside the DHS to strengthen the partnership between the public and private sectors and share best practices to thwart future attacks.

FireEye tops the Forrester External Threat Intelligence Services report

Forrester’s New Wave™: External Threat Intelligence Services, Q3 2018 report, published in September, has revealed that FireEye leads the field of 15 providers evaluated. The vendors surveyed are regarded as the most significant in the category.

The evaluation criteria:

- Surface web intelligence
- Dark web intelligence
- Technical intelligence
- Threat feeds
- Nation-state focus
- Cybercriminal focus
- Financial crime focus
- Vision and execution
- Global reach
- Strategic partnerships

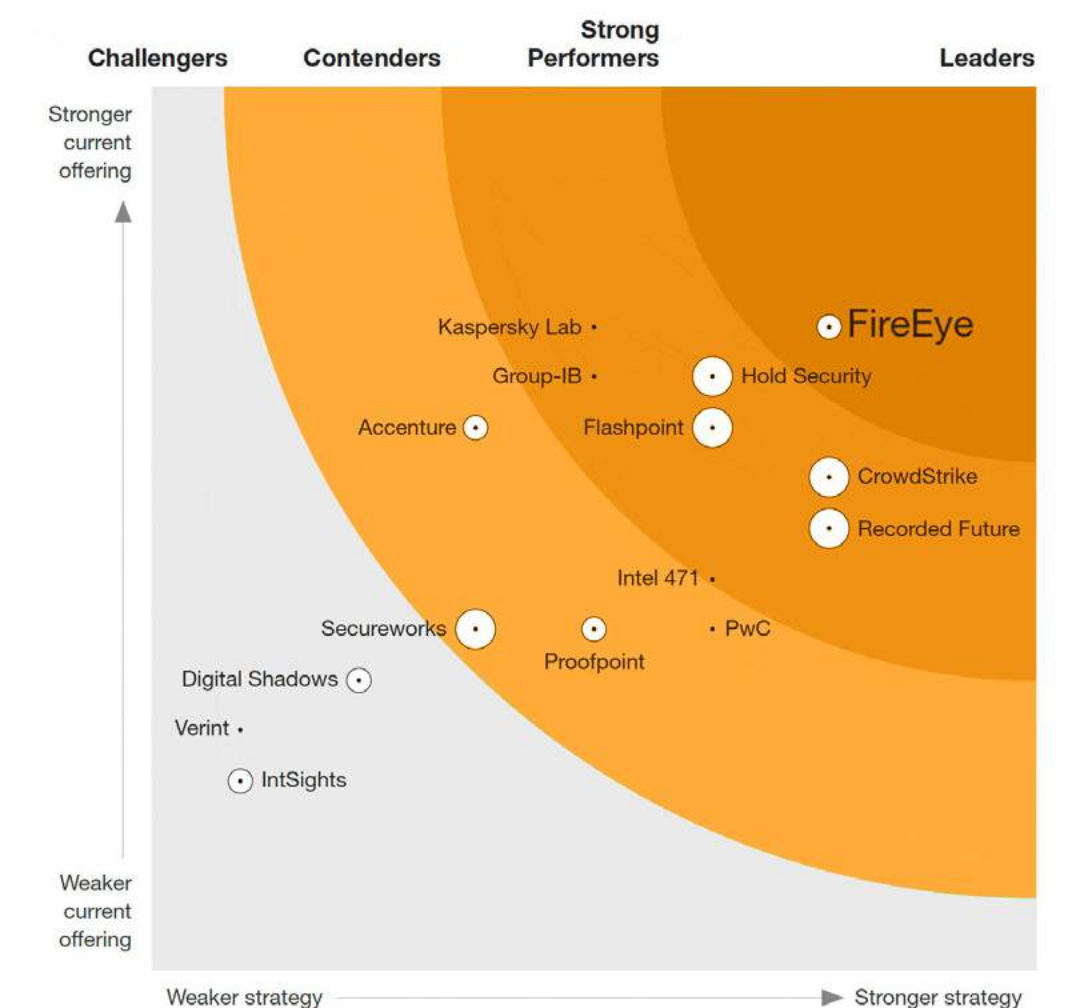
The report details Forrester’s findings about how each vendor scored against a number of criteria – and versus the other companies on the list – to assist buyers to make an informed choice about the most appropriate threat intelligence partners for their needs.

Why FireEye was #1

FireEye leads the pack with its collection capabilities. The importance of iSight Partners and Mandiant cannot be overlooked when assessing FireEye’s threat intelligence capabilities, which marry digital forensics, human intelligence (HUMINT), and a global sensor network.

The analyst’s New Wave series of reports evaluates emerging technologies based on a 10-criteria survey and two-hour briefing with respective vendors, selected on the basis that they have at least 75 enterprise threat intelligence customers, significant dedicated dark web collection capabilities and are frequently discussed by Forrester clients during inquiries and interviews. Vendors’ market presence and technical capabilities are also taken into account.

FireEye is the best fit for companies desiring a breadth of outcomes from a single vendor. Quilting together commercial vendors to accommodate your intelligence requirements can be a challenge. FireEye simplifies this process with an internationally recognized offering based on a wide collection capability.



Get ONE step ahead of email attacks

How It Happens

AN UNEXPECTED APPROACH

Cyber attackers use phone calls to help circumvent controls.



1 in 101 emails have malicious intent. We analyzed a data sample of over half-a-billion emails received between January and June 2018 to bring you the latest intel on – and trends in – both malware and malware-less attacks.

With only 32% of traffic seen in the dataset considered to be non-spam and free of malicious intent (and therefore suitable for the inbox) the other 68% is blocked or quarantined for a number of reasons. On the connection level, this is based principally on threat intelligence that identifies abnormalities in email traffic, namely a bad IP address or domain reputation, invalid Sender Policy Framework (SPF) record or non-DNS domain creation. On the content level, advanced threats such as malware and malware-less attacks encounter antivirus and anti-spam (AV / AS) engines, algorithms, Advanced URL Defense, Multi-Vector Virtual Execution (MVX) engine and increasingly, machine learning.

Email is every organization's most vulnerable vector, representing the point of entry for 91% of cyber attacks.

Malware and malware-less attacks

Cyber criminals constantly invent, and also evolve their attack techniques to bypass email security. A commonplace example of the latter in the US is W2 fraud. A W2 is an IRS form which must be filed by employers for every worker from whom income, social security or Medicare tax is withheld. Containing the name, address and Social Security number of the employee as well as the financial data, a compromised W2 represents an invaluable tool enabling a cybercriminal to file fraudulent tax returns (and claim the refund for themselves) or sell the information on the dark net. Emails attacks targeting accounting and human resources personnel designed, to socially engineer access to W2s, increase toward 15 April, the deadline for Federal income tax returns. After that date, attackers tend to switch to malware-based threats – normally in the guise of a refund notification but actually containing malicious links or attachments.

On average, 81% of all the malware-less attacks were categorized as phishing rather than impersonation attacks – understandable as the latter tend to be more personalized, requiring more effort on the part of the cyber criminal to make them plausible. Whilst phishing emails may be sent using a more scatter-gun approach, they are likely to be blocked by an email security service. The frequency of impersonation attacks over the six-month period scrutinized remained relatively constant, whereas phishing attacks continued to increase.

Impersonation Attacks

Impersonation attacks such as CEO fraud and business email compromise (BEC) have become increasingly popular for cyber criminals. Being text-based and appearing as innocent traffic, they represent quite a challenge for email security solutions. This places the onus on the employee to determine authenticity, which is why cyber criminals are frequently successful in persuading the recipient to comply with requests by using one or more social engineering techniques. One of these is the shift from domain name spoofing towards friendly name impersonation – simply changing the display/username rather than having to go through the process of buying and registering a domain name that can be confused with that of the target.

Conclusion

The data from the sample set highlights the importance of organizations investing in the protection of their weakest Achilles heel - email. Attacks continue to increase in volume and sophistication, using outside influences such as the tax season mentioned above, as well as appealing to basic human emotions to gain access to corporate assets. Effective protection requires multiple layers to succeed, not least an intelligence-led technical solution and employee education about the ever-present threat.

[Read the full report here >](#)

Keys to unlocking powerful cyber security

We take a look at FireEye and Gartner's unique webinar offering

Keeping abreast of tech has always been one of the greatest challenges for anybody in the IT sector. In cyber, it's no different

As examples, take new and evolving threat characteristics such as a 700% growth of ransomware families since 2016, the emergence and increase in crypto-mining rolling campaigns with attack waves, and a dramatic increase in nation state sponsored/endorsed targeted attacks – in terms of both complexity and the number of actors.

Facing and grasping these threats is formidable enough, but even more so in the face of the emergence of factors such as hybrid on-prem/cloud computing infrastructures and growing shadow IT estates.

To effectively keep pace with threats, organizations must apply a balanced approach

Comprising of the four key activities of incident lifecycle management: prevent, detect, respond to and predict threats. Critical considerations include outsourcing, security training, selection of efficient tools, workflow development and refinement, analytics and reporting, risk assessment and threat intelligence.

FireEye and Gartner have collaborated in the production of a unique webinar addressing precisely these issues. Gorka Sadowski, Gartner's Research Director, Security Infrastructure Protection and Christopher Porter, Chief Intelligence Strategist with FireEye, explore many of these topics in great detail to uncover the intricacies of cyber security success and options – including a presentation on FireEye ecosystem, operation, solutions and benefits to enterprises, including case studies and examples.



[View FireEye/Gartner webinar here >](#)

Suspected influence operation promotes Iranian political interests

Not all FireEye activity focuses on financial crime, espionage, threats against utilities, defense, CNI and the like.

Dispelling a widely-held belief that it is only Russia that engages in online, social media-driven influence operations for political ends, we have recently identified such an operation appearing to originate in Iran. Aimed at US, UK, Latin American and Middle East audiences since at least 2017, it conducts significant, wide-reaching activity promoting political narratives according to Iranian interests.

Leveraging a network of inauthentic news sites and social media on different platforms, the operation is aligned to Iranian political interests including anti-Saudi, anti-Israeli and pro-Palestinian themes, as well as promoting support for specific US policies favorable to Iran such as the nuclear deal (JCPOA). The

activity also includes significant anti-Trump messaging and the alignment of social media personas with an American liberal identity. It does not, however, appear to have been specifically designed to influence the 2018 US midterm elections as it extends well beyond US audiences and politics.

The report identifies and maps the registration and content promotion connections between the various news sites and social media account clusters identified to date, including detailed accounts of the websites concerned and the social media accounts connected with or otherwise promoting them. We have also identified Arabic-language, Middle East-focused sites that appear to be part of the broader operation.

[Read the full report here >](#)



North Korea's Un-usual suspects

A new emerging financially-motivated group that is an Advanced Persistent Threat (APT).

In our recent special report 'Un-usual Suspects', FireEye's intelligence takes a deep dive into the world of the financially motivated North Korean group APT38.

Responsible for destructive attacks against financial institutions, as well as some of the world's largest cyber heists, the group has attempted to steal in excess of \$1.1 billion, a figure based on widely publicized operations alone and therefore likely falls short of the actual sums involved.

We usually categorize financially-motivated actors as FIN groups. However, because this particular group is backed by, and acts on behalf of, the North Korean regime, we have categorized it as an APT. This nomenclature also reflects the fact that the group's activities are more akin to espionage: instead of simply obtaining accesses and moving to transfer funds as quickly as possible, APT38 conducts in-depth reconnaissance within compromised financial institutions balancing financially motivated objectives with learning about internal systems. We believe the group shares malware code and other development resources with a North Korean espionage group which we refer to as TEMP. Hermit.

Since at least 2014, the group has compromised more than 16 organizations in at least 13 different countries, sometimes simultaneously.

It is not just banks that are at risk from APT38, countries' financial governing bodies and media organizations with a focus on the financial sector have also been targeted. The key objective is to manipulate inter-bank financial systems to raise large sums of money for the Pyongyang regime, which is suffering increasingly severe international sanctions following continued weapons development and testing. This is also almost certainly behind the scale of and acceleration in APT38 activity – North Korea is desperate to obtain funds to pursue state interests.

An APT38 cyber bank robbery

This view is backed by published reports from defectors providing details on cyber-focused military units being tasked to generate income for the regime by engaging in piracy, freelance programming and other activities.

APT38 operations have become increasingly complex and destructive, with the adoption of a calculated approach which allows the sharpening of tactics, techniques, and procedures (TTPs) over time whilst evading detection. Given the sheer scale of the thefts they attempt, and their penchant for destroying targeted networks, APT38 should be considered a serious threat to the financial sector.

Our report provides a detailed account of the characteristics and operational specifics of APT38's extent of activities and modus operandi from initial compromise through internal reconnaissance, pivot to SWIFT servers, transfer of funds and destruction of evidence.

It throws light on the complexity of operations, including a toolset that includes at least 26 unique non-public and two publicly-available malware families with a variety of backdoors, disruptive tools, tunnelers and data miners, as well as the use of multiple evasion techniques such as modular malware and the use of false flags.

[Read the report here >](#)

APT38



34273894723094830293843427389472309483029384

34273894723094830293843427389472309483029384

APT38 global targeting



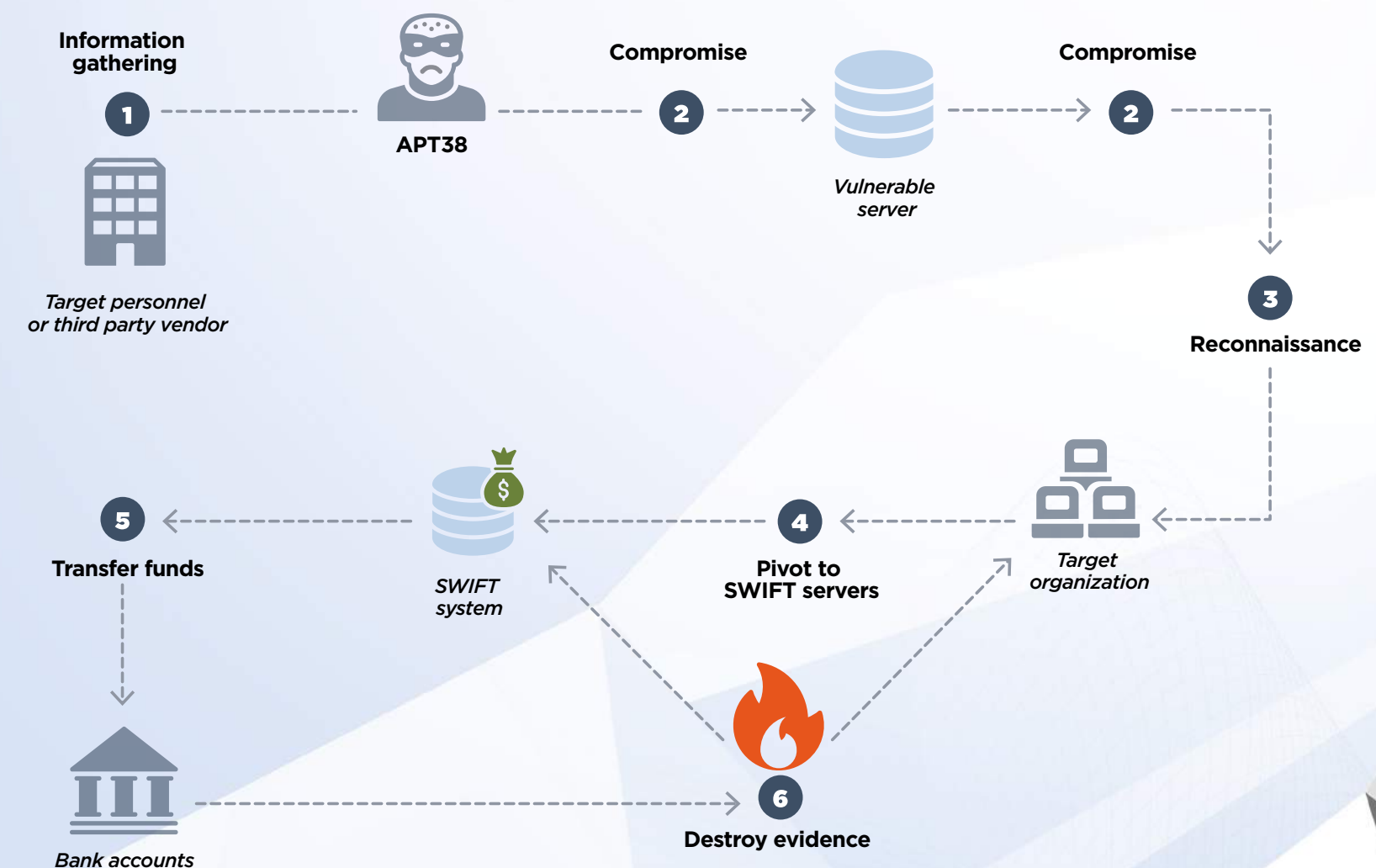
Industries targeted

- Banks/Credit Unions
- Media
- Financial Transaction
- Governments
- Financial Exchange

Categories of targeting

- Organizations targeted for infrastructure use
- Organizations targeted
- Both organizations and infrastructures targeted

A typical APT38 cyber bank robbery



Global webinar series



We have always found webinars to be an effective way to engage with cyber and other tech professionals – reaching the widest-possible variety of relevant roles across the globe with the maximum convenience to our audience. If you haven't seen it already, we invite you to watch our global webinar **Facing Forward: Cyber Security in 2019 and Beyond**.

As we look forward to the this year we wonder and what new tactics and strategies cybercriminals will develop, and whether their motives are financial, political, disruptive or economic. Two things are certain: attackers will attack and defenders will be tasked with stopping them. Another certainty, however, is that there is a lot more we can do to be prepared for upcoming threats and ensure we keep one step ahead. In this webinar, FireEye Chief Intelligence Strategist Christopher Porter shares his thoughts about cyber security in 2019, touching on various topics discussed in our Facing Forward: Cyber Security in 2019 and Beyond report including established and emerging nation state threats, how hostile actors are changing their tactics to stay ahead of defenders, and on a more specific vertical sector - threats to the aviation industry, including cyber espionage and cybercrime..

Register today to learn what lies ahead and stay one step ahead of cyber security threats.

Watch our recent global webinars

Over three days in October last year, we managed and hosted an unprecedented global online event for cyber professionals: a dozen webinars over three days, presented by senior FireEye experts, customers and market intelligence vendors.

The objective of the FireEye Cyber Resilience Virtual Summit was to convey real-time insights of the threat landscape from our latest investigations at the frontlines of cyber security, demonstrating how the combination of technology, threat intelligence and expertise can help you develop the cyber resilience you need.

Take a front row seat and watch at your leisure to find out about:

- Insights on the latest investigations from the frontlines of cyber security.
- Tools to gauge organizational readiness for a cyber crisis, as well as the best ways to determine what is needed to protect the company and its employees.
- 'Right-sized' security solutions that meet and evolve with evolving business needs.

Mapping Out a Battle Plan for Effectively Managing Cyber Risk

- [Evolving to an intel-led security organization](#)
- [Cyber security in today's IoT world](#)
- [Your breach readiness master plan: Take the sting out of a cyber attack](#)
- [What executives should know about Cyber AI](#)
- [FireEye global threat response – how we protect the world](#)

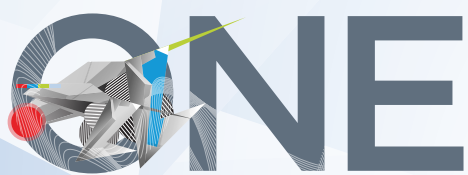
Gearing Up with Armor Against Cyber Crime

- [Responding to evolving threats with people, intelligence & technology](#)
- [Cyber security risk management – new methods to gain control](#)
- [How to elevate security as a boardroom priority](#)
- [Are you ready to handle a cyber crisis?](#)

Building 'Right Size' Security Solutions

- [Connecting the dots: The importance of an integrated security solution](#)
- [Cyber security in the financial sector \(expert panel discussion\)](#)
- [ICS landscape and Triton analysis \(autopsy of a real case\)](#)

 FIREEYE

 ONE

**ONE user receives one targeted email,
One click, ONE BREACH**

It only takes ONE. Discover more about email security
[fireeye.com/one](https://www.fireeye.com/one)

We hope you enjoyed this edition. Get the latest cyber security news from the frontlines by reading The Vision online.

[vision.fireeye.com](https://www.vision.fireeye.com)

Get in touch to find out how our security solutions can help protect your organisation.

contact-us@fireeye.com

www.fireeye.com

 FIREEYE