White Paper

Not ‘if’ but ‘when’: A data breach story in two parts

The value of next-generation intrusion detection in data breach response, investigation and mitigation

Introduction

What you need to know:

- Cyber-threats are on the rise but current point solutions and legacy IDS are expensive, clunky and unable to detect sophisticated attacks and lateral movement
- This paper details a typical data-stealing ransomware attack on a fictional financial services company (PremiumCredit), revealing two scenarios: the fall-out with and without next-gen IDS
- The holistic insight and advanced threat protection offered by next-gen IDS allows PremiumCredit to stop the attack in its tracks and respond quickly and effectively to mitigate risk
- Without this tooling, the firm is on the hook for major legal, regulatory and IT costs, and suffers reputational damage, customer attrition and share price devaluation

Today's IT and business leaders should be in no doubt: it's not a case of "if," but "when" you will suffer a serious cybersecurity breach. Over 8.4 billion records were exposed globally in Q1 2020, a 273% year-on-year increase.[1] The most important thing is having the tools at hand to react rapidly, understand exactly what has happened, and then remediate — managing financial and reputational risk as quickly and effectively as possible. Unfortunately, not all organizations have the technology and processes in place to make this a reality.

Supported by a cybercrime economy said to be worth as much as $1.5 trillion annually, the modern threat landscape is innovative and fast-changing.[2] One vendor alone blocked over 52.2 billion unique cyber-threats last year.[3] Yet this is only part of the story. Many more go undetected, in sophisticated multi-stage breaches using phishing, exploits of key infrastructure like RDP, living-off-the-land and fileless malware, credential stuffing and other techniques.

Attackers might perform months of reconnaissance on target organizations before striking. Once they have a foothold, they'll typically move laterally inside the network in search of prized data to steal. Many cybercrime gangs will then install ransomware and use the stolen data as a back-up plan in case the victim refuses to pay.

[1] https://www.riskbasedsecurity.com/2020/05/11/no-of-records-exposed-in-2020-q1-data-breaches-skyrockets-to-8-4-billion/
[2] https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf
[3] https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-sprawling-reach-of-complex-threats

Not fit-for-purpose

Organizations' efforts to tackle such threats are complicated by digital transformation, which has driven an ever-expanding corporate attack surface over recent years, and the failure of legacy security solutions to keep pace with underground innovation. The corporate network perimeter as we once knew it is gone. Today, sensitive data and IT systems extend from on-premises environments to the public cloud, BYOD devices, edge computing locations and IoT devices, supply chain networks and a new frontier of remote working endpoints, making the perimeter of today effectively "perimeter-less".

Traditional network security is no longer fit-for-purpose in this new era of digital growth, flexible working and sophisticated threats. Firewalls, AV, gateways and legacy intrusion detection systems (IDS) are point solutions unable to generate holistic end-to-end visibility and control. They lack the ability to spot lateral movement, internal attacks and the use of stolen or brute-forced credentials. Legacy IDS in particular is blighted by manual processes, high data logging costs, and detection issues. Today, the average time to identify and contain a breach is 280 days.[4]

Average time to identify
and contain a breach

280 days

[4] https://www.ibm.com/security/data-breach

A new approach

Instead, organizations need to leverage the power of machine learning enabled by network traffic analysis as part of next-gen, behavior-based IDS. Some, but not all IDS solutions, can provide the depth of insight needed for forensics that extends beyond initial detections for Network Detection and Response (NDR). Utilizing a solution with network traffic analysis that retains data economically in order to provide deep forensic capabilities offers more in terms of investigative workflows and remediation as well. This offers a smarter way to track suspicious actors across the entire IT environment by comparing it against baselined normal behavior. Thus, if the bad guys get in, you'll be able to spot them and take action rapidly to minimize the fallout.

To explain in more detail, this paper will walk the reader through a typical breach scenario from the point of view of a multinational financial institution. It will take you through a timeline from first incursion to discovery, forensics, and breach notification to regulators. But more importantly, it will describe what could happen with and without next-gen IDS powered by network traffic analysis — based on the perspective of key internal stakeholders: the CEO, CFO, Chief Legal Officer, and Heads of both IT and HR.

What happened? The PremiumCredit Corp story

PremiumCredit Corp is a mid-sized US financial institution with offices across Europe, North America and Asia. Like most organizations, it runs a combination of on-premises computing infrastructure and a hybrid public/private cloud environment. Most of its 8,000 employees are currently working remotely due to COVID-19 lockdowns in many of the markets it operates in, adding thousands more endpoints to the corporate network and plenty of strain to the bank's internal VPNs.

One vendor claimed to have detected 3.5 billon log-in attempts via credential stuffing over an 18-month period in the financial services sector alone.[5]

Unfortunately, even with advanced endpoint security tools in place, organizations like PremiumCredit are vulnerable to certain threat tools and techniques. It could be a simple phishing email that tricks a user into divulging their log-ins, enabling hackers to gain a foothold in the organization. Or it could be a covert brute force attack against an RDP endpoint.

In PremiumCredit's case, it is a credential stuffing attack utilizing previously breached email/password combos. Such lists are available in the millions on the dark web today.

One vendor claimed to have detected 3.5 billon log-in attempts via credential stuffing over an 18-month period in the financial services sector alone. Companies are exposed as much as individuals here because consumers often use their work email to register with third-party sites and sometimes share passwords across these multiple accounts.

Having bypassed the bank's endpoint and perimeter checks by impersonating a legitimate employee, the attackers are inside its North American corporate network. They swiftly set about moving laterally inside the network in search of sensitive data: this first stage of attack features internal reconnaissance, escalation of privileges and installing malware and tooling on specific machines. The suspicious east-west movement is immediately detected and flagged by PremiumCredit's NTA-powered next-gen IDS. A limited amount of employee data is exfiltrated before the bank's internal IT team "cuts the wire" to shut down the attack within just hours.

[5] https://www.akamai.com/uk/en/about/news/press/2019-press/state-of-the-internet-security-financial-services-attack-economy.jsp

Calling their bluff

The attackers have not managed to complete the first stage of mass data exfiltration or enter the second stage of the raid in which they would have begun encrypting data stores. However, undeterred, they contact PremiumCredit and claim to have a 17GB haul of customer and employee data which will be publicized unless a ransom is paid. They share a small sample of the data they did manage to steal as 'proof'.

However, thanks to their next-gen IDS solution, PremiumCredit has a precise forensic record of everything that happened on the network and what was taken. Thus, they are able to swiftly call the bluff of their attackers and notify the relevant authorities, internal stakeholders and data subjects of a minor incident.

The value of next-gen IDS

Legacy IDS systems have several crucial deficiencies, which mean they would most likely have failed to catch this attack until a large volume of PremiumCredit's data had been stolen and key systems encrypted with ransomware. They are unable to detect suspicious east-west activity, can't catch unknown threats (a critical differentiator between signature-based and behavior-based, next-gen IDS solutions), and don't provide complete visibility into the entire virtual environment.

Next-gen alternatives work differently. They examine 100% of transactions across network Layers 2-7 for total visibility, storing it in intelligent per-packet intel™, or metadata, to reduce capture and storage costs and prevent any performance impact. They are deployed via a SaaS model to make them viable in all IT environments, and have open integrations to further enhance threat intel and incident context. But perhaps most importantly, they feature advanced machine learning-powered analytics to support:

Statistical, behavioral, signature and anomaly detections

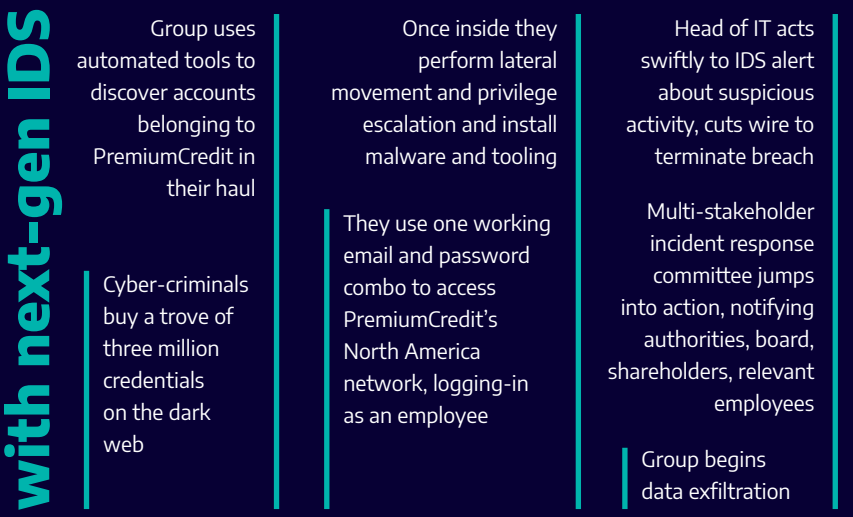
Detection, investigation, hunting, and alert management

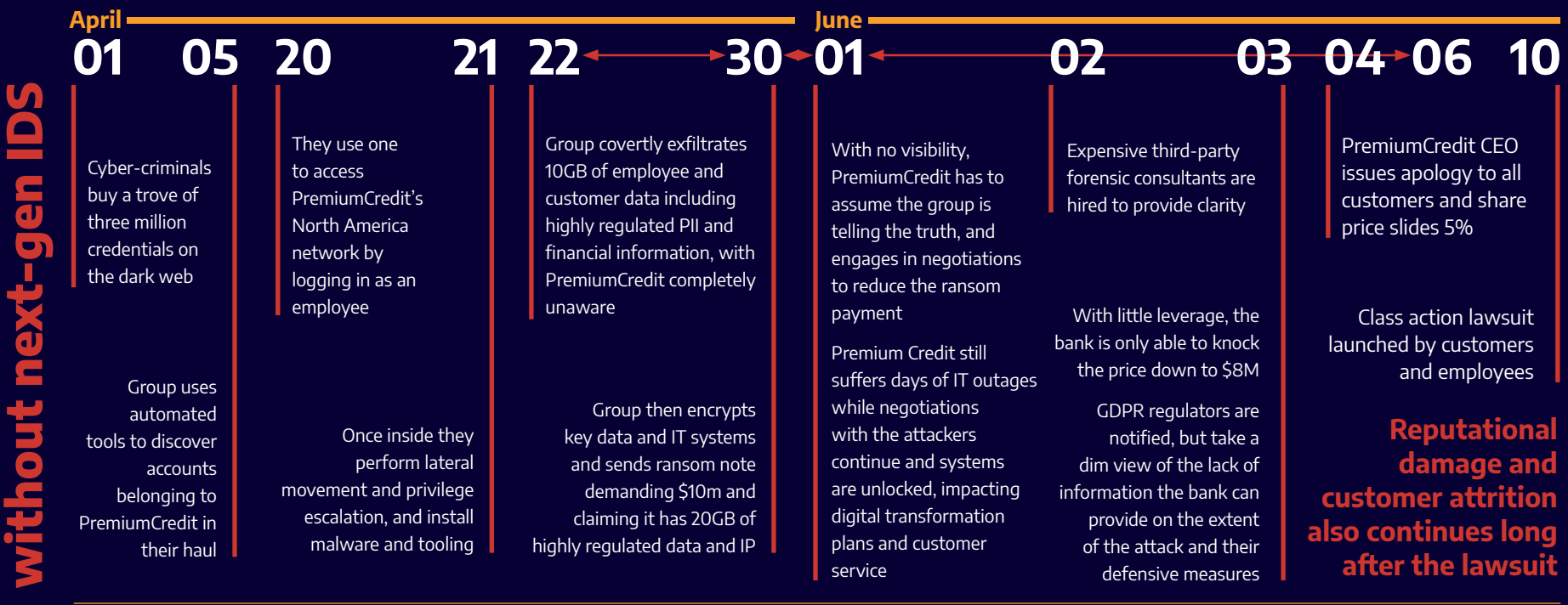
Early cyber kill chain warning signals for threats, Indicators of Compromise (IoCs), attacks, etc.

High fidelity forensic source data

This gave PremiumCredit a huge advantage in being able to spot suspicious lateral movement early on and take rapid action to remediate and recover.

Here are two alternative timelines, with and without next-gen IDS:





The view from the top

Here's what PremiumCredit's executive management team had to say about the incident, and what they would have had to say if the firm didn't have an next-gen IDS powered by network traffic analysis in place.

PremiumCredit's executive management team with next-gen IDS

"Speed and efficacy of decision making is the most critical thing for a CEO. You need to understand the worst-case scenario in any incident and prepare and react accordingly. **Having the insight we did turned what could have been the bank's darkest day into a mere minor blip.** I was able to reassure the board and our customers with prompt, accurate communication to minimize any financial or reputational impact."

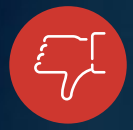
- PremiumCredit CEO

"I was able to react quickly to reach out to our insurer to talk through next steps. **My concerns over the financial impact of the breach were quickly allayed once it was clear we had caught the attack very early on with minimal data lost.** Thanks to this, the only major costs we incurred were in the extra man hours spent on managing the incident through to the end."

- PremiumCredit CFO

"Following any cybersecurity incident the most important thing is to have as much detailed info as possible at your disposal. **With this, the board can make the best, or at least most informed, decisions possible, and you are better equipped to make the necessary disclosures to the authorities.** We discovered that no EU citizens' data was obtained in our incident so there was no need to over-notify GDPR or other regulators in countries where we have employees, partners or customers."

- PremiumCredit CLO



PremiumCredit's executive management team without next-gen IDS

"**We were on the backfoot from day one, when our systems started to lock down due to the ransomware.** The hackers were in the network for over a week and we saw nothing. It's an enraging situation to deal with — we had to assume the worst in terms of data theft. It was almost impossible to manage reputational risk effectively with no clear picture of what had occurred. There will need to be big changes at a senior executive level going forward."

- PremiumCredit CEO

"**The financial impact on PremiumCredit has been disastrous.** Not only did we pay millions in ransom, we also spent significant sums on external attorneys, third-party forensics expertise, a ransom negotiator and IT support. Some, but not all, of this will be covered by cyber insurance, and we are expecting investigations and fines from regulatory authorities. The long-term financial impact of the breach may be severe if it impacts our ability to attract and retain customers."

- PremiumCredit CFO

"**Managing the fallout of this breach has been a huge undertaking from a legal and compliance perspective.** With very limited insight into what was taken, we had to assume the worst-case scenario in our notifications to the authorities which subsequently triggered regulatory investigations that will most likely lead to fines. It has also added hundreds of man hours in extra work for our legal team. We now have to deal with a class-action suit."

- PremiumCredit CLO

> From an IT perspective we couldn't have asked for more. Determined hackers will always find a way into your network, as they did here. It's how quickly you spot them and throw them out, and how effectively you remediate, that matters. The next-gen, behavior-based IDS solution we used was instrumental in ensuring our incident response ran like clockwork. **We contained the threat, remediated, restored the network and notified within hours.** And the forensics data we have will help us to build better defenses going forward."
>
> **- PremiumCredit Head of IT**

> **The wellbeing of employees is my primary concern, so it was a relief to discover that we stopped this attack before any significant personal information had been exfiltrated.** My role was therefore confined to merely identifying and notifying the handful of employees that had been affected."
>
> **- PremiumCredit Head of HR**

> **We were flying blind through the whole incident.** That gave the attackers time to move laterally, perform reconnaissance and steal what they wanted before encrypting our systems. Our legacy IDS and network security tools are too siloed, meaning we never got holistic insight into what was going on. The IT team has probably worked 10,000 hours remediating the incident and rebuilding our network, installing new VPNs and firewalls. That doesn't include the costs of contractors we had to bring in and project delays for growth-centric digital innovation initiatives, plus the realization that our back-ups were not all sufficient and that we lost some data."
>
> **- PremiumCredit Head of IT**

> Open, transparent communication with employees is vital after an incident of this kind. But the lack of visibility we had into what kind of data had been taken meant our crisis communications plan was difficult to action. **We have been forced to assume and communicate the worse-case scenario, expend significant resources on managing the fallout, spend significant dollars to put in place fraud-prevention services, and are predicting some impact on staff turnover."**
>
> **- PremiumCredit Head of HR**

The bad news

In short, without next-gen IDS, PremiumCredit would have likely suffered:

- Immediate financial impact from the cost of ransom, hiring third-party investigators, IT overtime, lost productivity and operational outages. Some estimates suggest global firms paid out tens of billions in ransom costs in 2019,[6] while network downtime could be as much as $300,000 per hour[7]
- Major reputational hit from non-compliance fines, lawsuits and the breach itself
- The financial cost of lawsuits and compliance fines. GDPR penalties could reach 4% of annual turnover, while the CCPA maximum is $750 per customer
- Customer attrition following a major data breach, and an unquantifiable impact to new customer pipelines
- Falling share price — declines hit an average of 7% in the fortnight following a breach and breached firms underperform the market in the long term, according to one study[8]

[6] https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/
[7] https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/
[8] https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/

Conclusion

The bottom line is that breaches are inevitable today. It's how you respond that matters: to your customers, employees, shareholders and regulators.

Skylight powered Security provides next-gen IDS enabled by network traffic analysis. Skylight's traffic analysis capabilities provide deep forensic capabilities with long-term high fidelity forensic data. We provide benefits across data collection, platform architecture, and advanced analytics:

Data. Rule-less Skylight software sensors collect intelligent per-packet intel, or metadata, to keep traffic capture and retention lightweight, a distributed approach covering modern threat surfaces more efficiently, reducing the performance and cost impact. Capable of handling network links of 10GB+, they capture 100% of transactions across network Layers 2-7 for comprehensive visibility across on-premises, remote, cloud, private DC, IoT and other environments.

Analytics. Skylight uses machine learning to provide statistical, signature, and anomaly threat and behavior detection. This enables: threat detection, investigation, hunting, and alert management; early cyber kill chain warning signals; and high fidelity forensic data. This provides visibility into lateral movement and unknown threats that traditional IDS and network security point solutions can't match.

Platform. Skylight's open architecture means it integrates neatly with third-party threat intelligence feeds, active directory, and other systems for added value. A SaaS deployment option means the platform is viable for all IT environments — cloud, on-premises data centers and hybrid — and can be activated in minutes.

About Accedian

Accedian is the leader in performance analytics, cybersecurity threat detection and end user experience solutions, dedicated to providing our customers with the ability to assure their digital infrastructure, while helping them to unlock the full productivity of their users.

Learn more at accedian.com

Accedian | 2351 Blvd. Alfred Nobel, N-410 | Saint-Laurent, QC H4S 2A9 | 1 866-685-8181 | **accedian.com**