A human approach to cyber security in banking

Understanding our adversaries

BANKING INSIGHTS

BAE SYSTEMS

Introduction

Attacks on financial institutions grew by 238% during the peak of the first Covid-19 wave last year as hackers took advantage of the pandemic as a distraction for their crimes, according to VMWare. The company reported that the rise in attack volumes coincided with major news events during the crisis, such as the first confirmed case in the US and the World Health Organization (WHO) declaring the pandemic, which were used as a lure for phishing emails. As the pandemic progressed, attacks also became more sophisticated as hackers gained greater understanding of financial institutions' internal policies, procedures and incident response blind spots.

To improve our chances of surviving such attacks, we must enhance our threat intelligence capabilities in order to understand, disrupt and mitigate the business risks such threats pose. However, this will require buy-in from chief information security officers (CISOs) and boards, and changes must be led by the threat intelligence industry itself.

What do we know?

By volume, the majority of the threats seen on a daily basis are automated, commodity attacks — "spray-and-pray" efforts are designed to catch out organisations and individuals who have obvious gaps in their defences. The real threat to businesses, however, comes from more targeted approaches, such as the "human-operated" or "hands-on-keyboard" activities seen in the evolution of ransomware attacks in recent years, and the motivated and persistent targeting by state-backed threat groups.

Ransomware operators have found a number of ways to grow the scale and speed of their attacks. Scanning for exposed Remote Desktop Protocol (RDP) logins, and exploitation of vulnerabilities in networking services are two popular techniques for gaining access, and tried-and-tested approaches using phishing emails also remain prevalent. Off-the-shelf pen-testing tools, such as Cobalt Strike and "living off the land" techniques, are used to blend in and move laterally. This allows the operators to remain undetected, providing the time needed to exfiltrate large amounts of data for "double extortion" attacks, and deploying ransomware across the victim estate. Recent cases have shown that these attacks can move from "end-to-end" in a matter of hours.

While the threat landscape was dominated by ransomware in 2020, a number of other developments have also been taking place. State actors have diversified their interests, and while sectors such as government and defence remain key interests, healthcare and Covid-19 responses have occupied a greater portion of their tasking.

Furthermore, "hacker-for-hire" groups, such as **Dark Basin**, also came to the fore in 2020. Such activity is increasingly commonplace, with groups such as these tasked to obtain login credentials and network access to targets in a range of sectors.

Dark Basin

AKA - Amanda Lovers

STATS

TYPE	Hacker-for-hire
FIRST OBSERVED	2015
VICTIMS	~1000s
OPSEC	Level 1
INNOVATION	Level 3
EFFECTIVENESS	Level 9
FAME	Level 8

FUN FACT

A hacking-for-hire outfit linked to a New Delhi-based IT company. Known to have phished extensively against political, energy, real estate and other targets.

BAEsystems.com/cyber

Where do we go from here?

Security experts often talk about the need for 'IT hygiene': best practices such as prompt patching, endpoint security and multi-factor authentication. These certainly play an important role, and the steps outlined by the National Cyber Security Centre (NCSC) and the government's Cyber Essentials scheme are a great place to start. Yet, best practice security will only get you so far, and time has also shown us how difficult it can be to "get the basics right" without leaving gaps.

To proactively enhance threat defence, you must understand the tactics, techniques and procedures (TTPs) of those seeking to harm your organisation. Threat intelligence is therefore a strategic necessity for a growing number and range of organisations across the financial services sector – including those who may not traditionally have thought of themselves as targets of motivated attackers. When done effectively, threat intelligence allows CISOs to be more proactive about security, stopping attacks before they've had a chance to cause serious reputational or financial damage. Threat intelligence can also help to improve resilience by enabling security teams to prioritise patches based on which vulnerabilities are being currently exploited.

A call for more intelligence sharing

However, there are some industry challenges which threaten to undermine an organisation's ability to reap these kinds of strategic benefits. On the supply side, the glut of threat intelligence offerings on the market – few of which offer a comprehensive range of capabilities – means those that can afford to often buy multiple overlapping solutions, while smaller peers aren't able to get complete coverage.

On the consumption side, many users of threat intelligence find it challenging to optimise their solutions. The result can see response teams chasing the wrong leads, or being flooded with alerts which they can't prioritise. In some cases, the data itself is too old to be useful.

Many in the industry are calling for more intelligence sharing. However, if systems were free and open to all comers, they could be more easily infiltrated by nation states and cyber criminals. On the other hand, if barriers are built around intelligence sharing organisations, those without economic clout may be left at a disadvantage. There are also persistent concerns that too much sharing could damage brand reputation.

These are difficult problems to solve, but one initiative offers some prospect for positive change. The Intelligence Network (a BAE Systems-backed body) is focused on helping safeguard society in the digital world by changing the way we think about cyber security. Its 2,000+ global members include cyber and financial crime professionals and industry influencers committed to creating a safer society. Seven crucial areas have already been ear-marked for change by 2025, and 'Understanding Adversaries' is right at the top of the list.

Considering the economic impact of the pandemic, which shows no signs of abating, a turbulent year lies ahead for the financial services sector. As such, now is not the time to take our metaphorical foot off the cyber-security pedal, with cyber-criminals constantly searching for signs of vulnerability.

By working together, we are confident we can drive change within the threat intelligence industry to improve our ability to understand adversaries, and make further progress in stopping them.

We are

BAE SYSTEMS

At BAE Systems, we provide some of the world's most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
19, Boulevard Malesherbes
75008 Paris
France
T: +33 (0) 1 55 27 37 37

BAE Systems
Mainzer Landstrasse 50
60325 Frankfurt am Main
Germany
T: +49 (0) 69 244 330 040

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

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

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai