NED MIG Presentation

Paul Taylor FREng
KPMG

May 2016

Threat Trends

APT

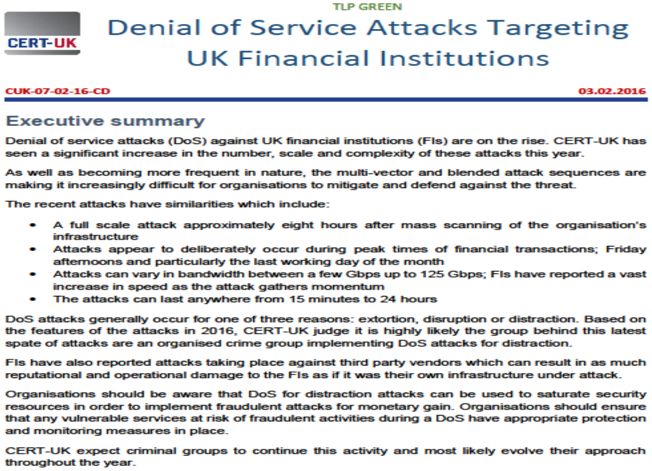
We have seen a continued move towards Advanced Persistent Threat style tactics from organised crime groups. Kaspersky reports METEL and GCMAN groups have been employing these tactics, plus the return of Carbanak malware.

Targeting treasury/finance/procurement

Increased targeting of corporate treasury, finance controller, and procurement functions has been observed. This is part of the ongoing pattern of CEO frauds and business email compromise frauds – a combination of social and technical attacks resulting in highly tailored spearphishing.

Changes in DDOS patterns

UK financial institutions have reported a change in patterns of Distributed Denial of Service attacks. Three institutions faced 46 separate attacks that were short duration and multi-vector. CERT UK released the below advisory.



TLP GREEN

CERT-UK

Denial of Service Attacks Targeting UK Financial Institutions

CUK-07-02-16-CD 03.02.2016

Executive summary

Denial of service attacks (DoS) against UK financial institutions (FIs) are on the rise. CERT-UK has seen a significant increase in the number, scale and complexity of these attacks this year.

As well as becoming more frequent in nature, the multi-vector and blended attack sequences are making it increasingly difficult for organisations to mitigate and defend against the threat.

The recent attacks have similarities which include:

- A full scale attack approximately eight hours after mass scanning of the organisation's infrastructure
- Attacks appear to deliberately occur during peak times of financial transactions; Friday afternoons and particularly the last working day of the month
- Attacks can vary in bandwidth between a few Gbps up to 125 Gbps; FIs have reported a vast increase in speed as the attack gathers momentum
- The attacks can last anywhere from 15 minutes to 24 hours

DoS attacks generally occur for one of three reasons: extortion, disruption or distraction. Based on the features of the attacks in 2016, CERT-UK judge it is highly likely the group behind this latest spate of attacks are an organised crime group implementing DoS attacks for distraction.

FIs have also reported attacks taking place against third party vendors which can result in as much reputational and operational damage to the FIs as if it was their own infrastructure under attack.

Organisations should be aware that DoS for distraction attacks can be used to saturate security resources in order to implement fraudulent attacks for monetary gain. Organisations should ensure that any vulnerable services at risk of fraudulent activities during a DoS have appropriate protection and monitoring measures in place.

CERT-UK expect criminal groups to continue this activity and most likely evolve their approach throughout the year.

Threat Trends

Botnets attacking e-commerce

Evidence has been discovered of botnets being used to target e-commerce and corporate targets. We are increasingly seeing targets that are smaller and less well protected than typical banking targets.

Russian action to disrupt Dyre group

There has been initial evidence to suggest Russian action taken to disrupt the Dyre organised crime group in Moscow. This could be interpreted as concerted action against groups such as this given recent attacks on Russian banking interests.

Ukraine power grid attacks

Experts suggest that the recent attacks on the Ukrainian power grid would be easily replicated across the UK and many other nations as equipment, systems, and processes are similar. The attacks began with phishing emails that deposited BlackEnergy 3 malware on machines which gathered login credentials in the background, allowing attackers to later login in remotely and gain control.

Regulatory Concerns

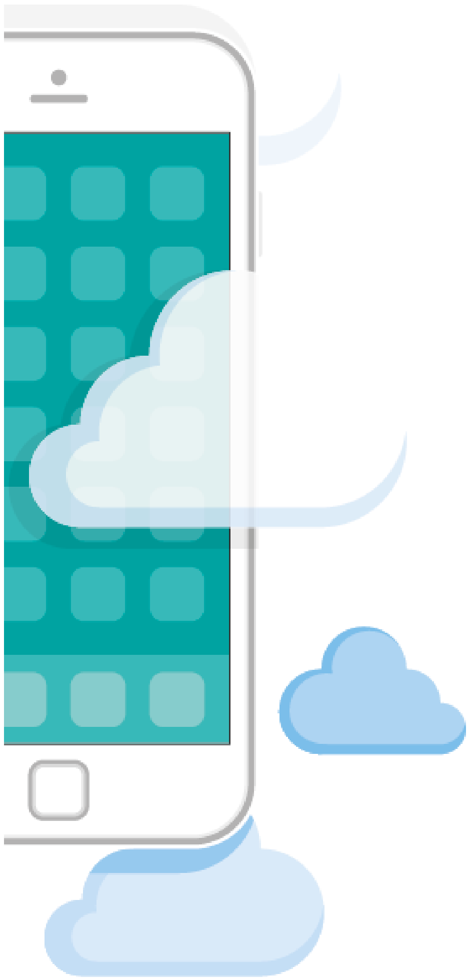
Privacy Shield

Privacy shield agreement provides a potential counter to the collapse of the safe harbour arrangement but there is growing pressure on cloud providers and vendors to demonstrate effective data privacy measures. This is directly linked to forthcoming EU general data protection regulation.

EU Network and Information Directive

EU Network and information directive is nearing approval. However, this will fire the starting pistol for two years of translation into national legislation on security standards, incident handling and disclosure. Organisations will then need to embed within their own practices and policies in whatever way they can to meet the regulatory pressure.

Technology



- Banks are continuing to explore Blockchain technologies. This includes investments by Bank of America and JP Morgan, and European Central Banking testing of blockchain technology to improve bank security payment systems.
- Multiple retail banks signal intent to roll-out biometric authentication mechanisms for mobile banking customers including use of voice, fingerprint and facial recognition. There is even a trial of heartrate recognition. FinTech startups are also exploring behavioural biometric solutions.
- We are seeing a general trend towards adoption of public cloud offerings across the financial services industry.

Board Level Awareness

Board level awareness of emerging cyber threats and direct involvement in determining the response is critical. Threat intelligence can help organisations become more proactive, focussed and preventative to take control of cyber risk in a unique and positive way. Asking the questions below, can help leaders quickly identify gaps in the current cyber security strategy and encourage an organisation-wide approach to securing the future of their business.

- How do we move from **reacting to anticipating** cyber attacks?
- How do we put the cyber threats we face into a **business context**?
- How do we **demonstrate the return on investment** of our cyber security measures.

- When was the cyber threat **last examined** by the Board?
- Is cyber part of the Board's **strategy discussions?**
- Does our CIO **know when to act** and are they empowered to do so? Has it been effective?

Board Level Awareness

Boardroom Questions

- Who in our organisation is responsible for cyber security issues?
- What are our key information assets?
- Do we fully understand our current vulnerabilities?
- What is our risk appetite?
- Do any of our supply chain partners put us at risk?
- Does my organisation meet all of its obligations for information assurance?
- Do we meet the information security requirements to bid for government contracts?
- What processes do we have in place to deal with cyber threats?
- Are our competitors ahead of us? If so, does this give them an advantage?

Questions for Senior Management

- What should our response be?
- How effective has our response been?
- What do you know about the people / organisations responsible for the attacks and how do they operate?
- Are there any patterns regarding cyber attacks that make our information and assets more vulnerable at certain times?
- Who should we be sharing threat intelligence with and how?
- How do we establish an effective Security Operations Centre?
- How can we use security as a business enabler?

KPMG

Thank you

Contact:

Paul Taylor FREng
Partner, UK Head of Cyber Security
Risk Consulting
T: + 44 (0)20 7311 2164
E: paul.taylor@kpmg.co.uk