TIME TO ADAPT ?

MAY 2023

THE RISE OF ADVANCED PERSISTENT THREATS

PRESENTED BY
GATEWATCHER

RESEARCH AMONGST EUROPEAN BUSINESSES TO ASSESS THE CURRENT STATE OF APT AND THE RESPONSE IN ENTERPRISES.

RESEARCH CONDUCTED BY
VANSON BOURNE

GATEWATCHER

CONTENT_

01 INTRODUCTION

02 THE RISE OF ADVANCED PERSISTENT THREATS

03 APTs: LACK OF VISIBILITY AS A RISK

04 IDENTIFYING THE SIX MAIN SECURITY CHALLENGES IN EUROPE

05 SOLUTIONS AND TECHNOLOGIES FAVOURED BY EUROPEAN COMPANIES

06 APTs AS THE NEW NORMAL IN CYBERSECURITY

07 METHODOLOGY

08 ABOUT

01

INTRODUCTION_

It is an uncomfortable truth that threats evolve. To survive, bad guys must get better at being bad guys.

And in the case of cyber security, that evolution is often faster than the good guys – the reality is that security teams are all too often, playing catch up. The latest iteration of this evolution is the maturation of the advanced, persistent threat, or APT.

Commercialised definitions of APT already abound as many vendors have begun to orientate their technologies towards this threat. The 'original' and most comprehensive definition can be found in the NIST Special Publication Managing Information Security Risk, which defines APTs as:

"An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organisations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organisation; or positioning itself to carry out these objectives in the future."

The advanced persistent threat :

- pursues its objectives repeatedly over an extended period of time;
- adapts to defenders' efforts to resist it;
- is determined to maintain the level of interaction needed to execute its objectives. [1]

In other words, **APTs are characterised by intelligent, stealthy attacks that are patient, persistent, intelligent, well-equipped and focused.** They are the polar opposite of hacking a Twitter account or an attempt at a digital 'smash and grab' of user details.

While advanced persistent threats are characterised by attacks that are focused, initial phases often obscure the true target. Some examples include the attack on unprotected VMware ESXi servers around the world in February 2023 - a large-scale ransomware attack with more than 3,200 servers compromised in Europe , the US and Canada. In January 2023, a misconfigured Microsoft application allowed anyone to log in and modify Bing.com search results, endangering the accounts of Office 365 users. Most recently, in March 2023, legitimate versions of the 3CX DesktopApp were compromised and exploited by hackers in order to jeopardise more than 600,000 companies using the app.

As such, APTs typically occur in the context of cyber espionage, co-ordinated hacktivism, financial cyber crime or as part of an organised attempt to destroy the digital capabilities of a given organisation. **But, as with all criminal enterprises, APTs have spread into the business mainstream.**

Source

[1] *NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011*

02

THE RISE OF ADVANCED PERSISTENT THREATS_

In recent years, many studies and organisations have highlighted the increase in APT threats towards certain sectors. For example, the COVID-19 pandemic has led to an increased nation-state activity from APT groups targeting healthcare and essential services, as identified by CISA and NCSC[2]. Furthermore, CERT-EU has also observed that the number of APT attacks against EU institutions, bodies and agencies (EUIBAs) increased by 60% in 2020 compared to 2019[3] . Perhaps the most telling sign of the rise of APTs, has been the evolution of the APT protection market, which is expected to exceed 15 billion U.S. dollars by 2026[4].

This research project began in the light of these developments and following trends seen in Gatewatcher's own cyberthreat intelligence capability and as part of its active monitoring of cyber threats. As a result, we looked to assess pan European readiness and response to these threats.

There is certainly substantial APT activity in businesses throughout the markets we surveyed. Across the UK, France and Germany, 93% of the enterprises surveyed are currently engaged in the detection and discovery of APTs. These figures are broadly consistent within each individual country and regardless of the size of company.

Addressing the APT threat seems to be predominantly an in-house operation. Throughout the countries surveyed, 19% currently outsource their APT response to a services provider or MSSP. This did increase slightly for France, where 23% of companies use a partner for APT protection.

Sources

[2] *Joint alert from the DHS, CISA and the NCSC, APT Groups Target Healthcare and Essential Services, January 25, 2022*

[3] *CERT-EU, Threat Landscape Report, June 2021*

[4] *Statista, Mars 2022*

WHEN THINKING ABOUT ADVANCED PERSISTENT THREATS, WHICH OF THE FOLLOWING STATEMENTS IS MOST TRUE FOR YOUR ORGANISATION ?

25%

We seek to detect and discover APT but face challenges identifying the method of entry.

21%

We seek to detect and discover APT but face challenges supporting the technology.

15%

We seek to detect and discover APTs but face challenges remediating the attack.

03

APTs: LACK OF VISIBILITY AS A RISK_

When asked to address the specific issues surrounding APTs and how they might compromise the security posture or their organisation, just under half (47%) of respondents identified a lack of visibility throughout the network as a key factor, whilst another 40% disclosed a lack of the necessary skills within their security teams.

A further 35% also mentioned gaps in current endpoint provision and nearly a third (30%) cited false positive and the subsequent alert fatigue as a source of security compromise. Reflecting the increased awareness of the importance of securing the supply chain, 29% identified third-party subcontractors that are connected to an organisation's systems as a source of APT threat.

Across Europe, 25% of respondents currently seek to detect and discover APTs but face challenges identifying the method of entry. A further 21% face challenges supporting the technology (although there is a notable increase here for Germany, as 30% of respondents cited such issues). Throughout all the markets surveyed, 15% face challenges remediating APT attacks.

Just under 1 in 5 respondents currently outsource their protection against APTs. Increased vigilance must be shown with this protection as 28% of respondents thought poor communication from a service/ security service provider led to APT-based compromises of their security posture.

04

IDENTIFYING THE SIX MAIN SECURITY CHALLENGES IN EUROPE_

The survey also identifies six security challenges ranked by risk level. Across all three markets, the cyber crime threat of individual bad actors, such as independent black hats, hacktivists or script kiddies is seen as the most pressing cyber security challenge faced by organisations, identified by 54% of respondents.

This was closely followed by the threat of data loss, identified by 51%. Ransomware remains a key issue, cited by 47%. Cyber crime threats posed by nation-states was identified by 38% of respondents throughout Europe, with just over a third (34%) naming industrial espionage as the top concern. Internal threats such as disgruntled employees were top of mind for just 28% of respondents.

The study also points to differences in perception between British, French and German decision-makers. In France, data loss tops the list of concerns (65%), while individual hackers rank first in Germany and in the UK (62% and 52% respectively). Ransomware is also the second biggest concern for German IT decision makers (52%), compared to 47% and 43% in France and the UK.

WHICH OF THE FOLLOWING MOST ACCURATELY DESCRIBES THE MOST PRESSING CYBERSECURITY CHALLENGES YOUR ORGANISATION FACES ?

55% OF RESPONDENTS NAME NETWORK DETECTION AND RESPONSE **-NDR-** AS A TOP TECHNOLOGY THAT THEIR ORGANISATION USES TO DEFEND AGAINST APTs.

05

SOLUTIONS AND TECHNOLOGIES FAVOURED BY EUROPEAN COMPANIES_

When it comes to the technologies being deployed against APTs: endpoint detection and response (EDR) and firewalls top the choices across all three markets, identified by 62% and 57% respectively.

Security Information and Event Management (SIEM) and Network Detection and Response (NDR) follow closely with 56% and 55%. Rounding out the top five technologies levelled against the APT threat is Extended Detection and Response (XDR) with 38%.

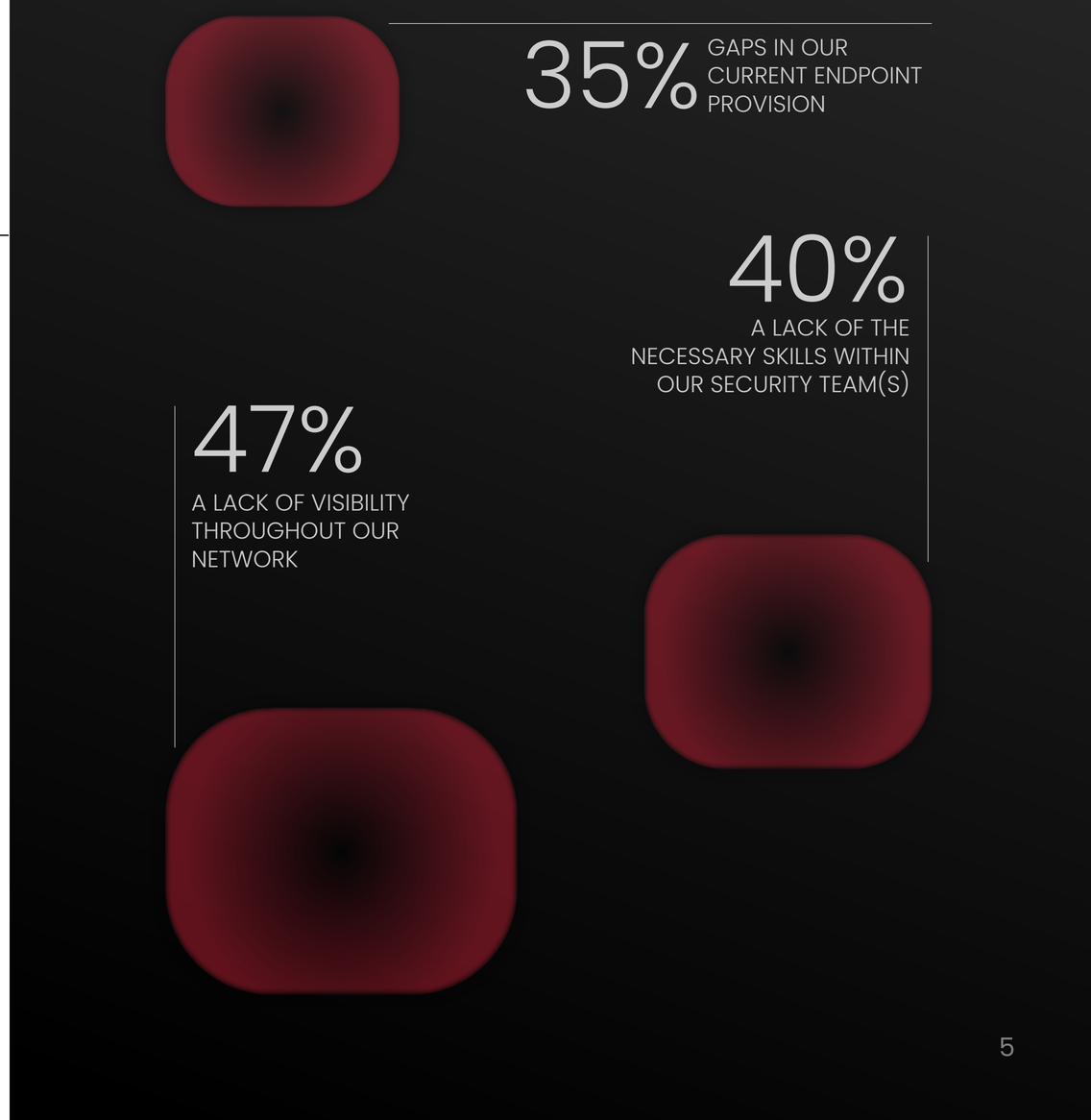
NDR continues to catch the interest of many companies facing the APT threat: the NDR market is set to reach approximately $5.4bn by 2028[5], with a projected compound annual growth rate (CAGR) of 13.7% during 2022-2028. This reflects not only the increased awareness of the technology, but also its implementation as part of the well-known 'triad' of cybersecurity, fusing EDR, SIEM and NDR.

This combination of technologies is a welcome response to the APT threat. When asked – with specific regard to APTs - what they believe most compromises their organisation's security posture, 47% of respondents across the three markets identified a lack of visibility – and again, this is something that NDR addresses specifically. This technological concern was followed by that most pressing but perennial of industry issues – expertise: as 40% identified a lack of skills within their teams.

In this light, the increased visibility of NDR and the focus on EDR makes a great deal of sense, especially when combined with the automation offered by some firewalls. By supporting rapid investigation, internal visibility, intelligent response, and enhanced threat detection, NDR works so well because it's extremely difficult for threat actors to hide their activity at the network layer.

Sources

[1] *Industry Research, Global "Network Detection and Response (NDR) Market" Research Report 2022-2028 (Press release), June 2022.*



06

APT AS THE NEW NORMAL IN CYBERSECURITY_

The main concern with cyber threats is often the identification of the bad actors. Whilst it is inherently difficult to get an accurate picture of successful APT "bad guys", because part of their modus operandi is to remain as hidden as possible for as long as possible, the research did seek to identify the biggest threats as perceived by IT decision makers across the three markets. As part of these questions, we included categories that typically represent those criminals most likely to deploy APT methodologies.

This research shows that businesses are still relying heavily on endpoint protection, whilst recognizing that it is visibility across the network that is now needed to address APTs. This also reveals the encouraging and growing awareness among organisations for network technologies – such as NDR - which will become the preferred solution for protecting organisations in the future.

The development and evolution of advanced persistent threats has created an ecosystem that rewards criminals able to exercise patience, insight and logic.

As such, this threat demands a response from the cyber security industry that is the equal of a more sophisticated protagonist – a response that needs to combine increased visibility, a wider presence throughout the network and a more circumspect, probing attitude that looks for the early signs of larger, longer-term attacks.

In short, it is now time to evolve: organisations and enterprises need to adapt their approach to the threat landscape and see APTs as the new normal in cybersecurity.

07

METHODOLOGY_

For the study, commissioned by Gatewatcher, research specialist Vanson Bourne carried out a survey between January and February 2023 amongst 300 senior IT decision makers across UK, France, and Germany. The 300 respondents come from the following sectors: IT, technology and telecoms, Financial services, Retail, distribution and transport, Manufacturing, Business and professional services, Other commercial sector. 204 respondents belong to companies with 3,000 or more employees; the remaining 96 IT decision-makers belong to companies with 3,000 to 1,000 employees.

ABOUT THIS SURVEY

COUNTRY OF RESPONDENTS

UK
100

FRANCE
100

GERMANY
100

DISTRIBUTION OF RESPONDENTS BY COMPANY SIZE

TOTAL
300

3 000 OR MORE EMPLOYEES
204

1 000 - 2 999 EMPLOYEES
96

SECTOR OF RESPONDENTS

300 SENIOR IT DECISION MAKERS ACROSS THE FOLLOWING SECTORS :

IT, TECHNOLOGY AND TELECOMMUNICATIONS
72

FINANCIAL SERVICES
67

RETAIL, DISTRIBUTION AND TRANSPORT
48

MANUFACTURING
41

BUSINESS AND PROFESSIONAL SERVICES
17

OTHER COMMERCIAL SECTOR
55

08

ABOUT_

GATEWATCHER

As a technology leader in cyber threat detection, Gatewatcher has been protecting the critical networks of large enterprises and public institutions since 2015. Gatewatcher's solutions combine AI with dynamic analysis techniques to provide a 360°, real-time view of cyber threats across the entire network, in the cloud and on premise.

www.gatewatcher.com

VANSON BOURNE

Vanson Bourne is an independent and trusted market research partner, specializing in technology. Vanson Bourne delivers data and insights for marketing content and contribute to the global success of some of the world's biggest technology companies. Vanson Bourne offers support through the entire research process, with expertise in sampling, questionnaire design, project management, and data interpretation and analysis.

www.vansonbourne.com