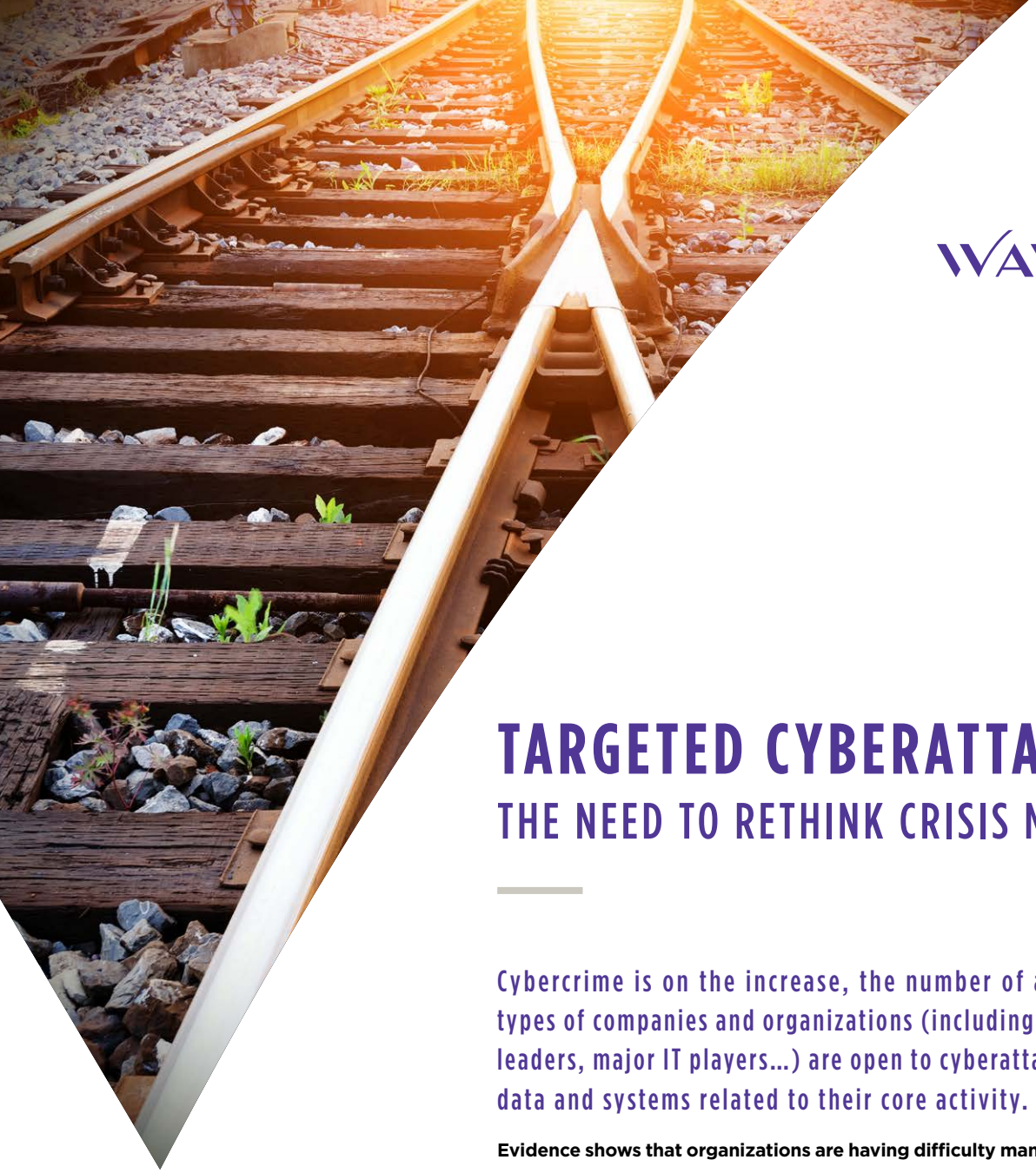

WAVESTONE

TARGETED CYBERATTACKS

THE NEED TO RETHINK CRISIS MANAGEMENT

Cybercrime is on the increase, the number of attacks is growing. All types of companies and organizations (including government, industrial leaders, major IT players…) are open to cyberattacks that directly target data and systems related to their core activity.

Evidence shows that organizations are having difficulty managing this new type of crisis. Intruders often penetrate the company and then move in «quietly» so that they can directly steal confidential data or plan their attacks without disrupting the apparent functioning of the company's IT systems. These intrusions are difficult to identify, to deal with and ultimately to remedy in a definitive manner.

This gives rise to three questions: How does one react to these attacks? What steps must be taken and organizations set up to best prepare for these attacks? What actions should be undertaken to change the situation?

FROM COMMON CYBERCRIME TO TARGETED ATTACK

Trends in hacker motivation have evolved considerably over the past few years. At first, attacks were carried out by isolated individuals seeking to make a reputation for themselves by proving they could overcome technical challenges. The majority of attacks are now being carried out for ideological, lucrative or political reasons. Examples include targeted leaks of sensitive information (such as in the AshleyMadison hack), denial of service attacks (conducted by groups such as Anonymous and LizardSquad like the one that impacted Sony and Microsoft gaming platforms), personal and financial data theft (JPMorgan Chase, Target…), infrastructure and government-data attacks (French Ministry of Finance, Office of Personal Management in the US, etc.).

AUTHORS

GÉRÔME BILLOIS
gerome.billois@wavestone.com

FRÉDÉRIC CHOLLET
frederic.chollet@wavestone.com

There are three major categories of attack:

The first of these, **dispersed attacks**, are not target-specific or are directed at the general public (viruses, phishing, ransomware, etc.). These attacks are easily countered by using standard security mechanisms.

The second category concerns **opportunistic attacks**. Technically more advanced than the first category, these attacks target organizations that are the least secure, with a view to reaping immediate rewards (personal and credit-card data theft, etc.). Most of these attacks can be avoided by implementing and maintaining a standard security mechanism. Because intruders look to make fast gains, they will readily switch target whenever they encounter difficulties carrying out an attack.

The third category, **targeted attacks**, is currently experiencing an uptick in their activity. These attacks specifically target the sensitive information or systems of the organization in question. The main most common objective here is to steal confidential data; the scenario upon which we have based this analysis. At the same time, destructive attacks have emerged, albeit in considerably fewer numbers.

During a targeted attack, infiltrators take time to analyse the aimed organization, prepare their attack scenarios and use the technical and human means at their disposal, both simple and complex, to attain their objective.

Technical levels and the means available can increase drastically. The security community talks about the *Advanced Persistent Threat* (APT) when referring to potential threats of this nature that today represent a real challenge, particularly for crisis management.

TARGETED ATTACKS: A SILENT MENACE WITH DELAYED IMPACT

These targeted attacks are undermining standard crisis-management and security-incident management processes for several reasons:

- **The attacks are silent:** intruders use the most discrete attack mechanisms to conceal their presence. Data can be exfiltrated via encrypted tunnels or attacks can be carried out outside normal business hours. The figures are staggering: the average time it takes to detect an attack is around 150 days. (*Mandiant 2016 M-trends report*).
- **Perpetrators are efficient and quick:** intruders are organised into structured teams of “experts”, who gain access to, and maintain control of the IT system, “explorers”, who locate the targeted information, and “workers”, who extract the data. With this organization, it is often possible to carry out attacks more rapidly than the time it takes for major organizations to react. The latest Verizon cybercrime report clearly shows that nearly 90% of attacks are successfully conducted in under an hour, and 67% of data-extraction is carried out in less than twenty-four hours.
- **The effects of these attacks are not very apparent:** data theft and extraction do not disrupt the day-to-day operations of the company and the IT System continues to function correctly. If no advanced surveillance tools are in place, the existence of an attack may still be discovered, although usually by accident - a stroke of luck - or because external consequences are already perceptible. The numbers support this: 53% of targeted attacks are detected by a third party (*Mandiant 2016 M-trends report*).
- **These attacks are aimed at securing a long-term position in the IT system:** Evidence shows that after breaking into an IT System, hackers seek to maintain control of the system by compromising the various IS components globally. Taking control of centralized management systems (in particular the Active Directory) is also very common. The elements that have been attacked are often compromised many times over to complicate the cleaning and remediation process.

Today, major organizations have implemented incident-management procedures that deal with standard attacks, such as viruses, ransomware, phishing, and even DDoS (distributed denial of service), etc.

The targeted-attack paradox: a different time scale between the moment of attack and time of detection

Source: Wavestone, Mandiant, Verizon - 2016

These processes often function in a uniform manner whereby an incident triggers an analysis and resolution, without necessarily trying to establish if the incident is part of a larger attack.

Crisis management is, above all, a management tool. These mechanisms are designed and implemented to address major «disruptive» events which interrupt or modify the daily functioning of the organization. This is not the case for most of the targeted attacks!

What can therefore be done to address discrete, progressive incidents that do not have a direct impact on a company’s business but do compromise data confidentiality and information system integrity?

REDEFINING THE FUNDAMENTALS OF CRISIS MANAGEMENT

A targeted attack is not an IT crisis but a business crisis

Because the purpose of these attacks is to steal or alter business data and systems, companies must involve their business divisions and identify their current business challenges (major contracts, mergers/acquisitions, R&D, etc.) to be able to anticipate potential targets of attack and react in a proactive manner. In the same vein, and depending on the context, support from government bodies may also be sought. Despite their vigilance, information security teams cannot be attentive on all fronts because the scope of observation of the IT System is often too wide. Identifying key business targets makes it possible to focus on sensitive areas.

Increasing ones visibility on IT systems is essential

Analysing attacks and proposing efficient counter measures requires detecting and connecting series of isolated incidents and suspicious events. To achieve this, it is essential to mobilise teams of forensic experts and gain an understanding of how the malicious codes used for the attack actually work so as to be able to propose relevant technical action plans. These resources, currently in sparse number, should be rapidly mobilized.

Access to tools designed to detect “early signs” of cyberattack (log analysis, SOC/SIEM, network probes and intrusion detection) is also a real asset, although, unfortunately, their use has not, as yet, been generalised. Our experience shows that while it is possible to deploy this type of tool rapidly during a crisis, a considerable degree of expertise is required for it to be efficient.

Access to tools designed to detect “early signs” of cyberattack (log analysis, SOC/SIEM, network probes and intrusion detection) is also a real asset, although, unfortunately, their use has not, as yet, been generalised. Our experience shows that while it is possible to deploy this type of tool rapidly during a crisis, a considerable degree of expertise is required for it to be efficient.

In addition, enhancing the sensitivity of IT teams to detect suspicious behaviour (partial malfunction, increase in storage volumes and network flows, etc.) and developing the ability to automate analysis and remediation for the most common incident are another interesting approaches. Information concerning the major elements of an intrusion can be gathered from these filed level details and subsequently used to analyze the scope of the attack and detect the potential risk areas.

Multitude of silent and misleading attacks demands pulling back and think twice

Despite the multitude of events, it is important to step back at regular intervals and think of the situation so as to understand the purpose of the attack, how it develops and define a solution. As such, to achieve the required level of objectivity, the steering team should be separate from on-the-ground operational teams.

Caution is also warranted with regard to the logic of diversion, a tactic often used by intruders (for instance an attack on other less critical servers, etc.). In these situations it is advisable to stay focused on the potential targets defined in conjunction with the business divisions and remain vigilant during periods of corporate inactivity (after-hour periods, week-ends and public holidays).

> « Targeted attacks are not IT crises but business crises carried out for the purpose of stealing business data »

One constraint often encountered in such crisis situations is the disproportionate amount of decision makers mobilised relative to the small number of operational players capable of carrying out the actions required. The duration of these attacks (sometimes lasting several weeks, even months) requires adopting a different pace from that used in dealing with standard crises. A long term crisis organization must be set up with alternating teams to ensure round-the-clock monitoring.

Access to a parallel and independent emergency IT System

Experience shows that perpetrators often succeed in taking over control of the Active Directory or the email messaging system which enables them to «listen in» on, and anticipate the decisions made by the organization’s crisis unit. To be able to react efficiently during a crisis, organizations must use workstations other than those used for standard administration purposes and install a specific messaging service. Using Cloud services is a possibility. Caution is however warranted since hackers can also compromise the personal accounts of some employees.

Acknowledging loss of confidence in the IT System and winning it back

The discovery of a major intrusion can often trigger a loss of trust in an organization’s IT System depending on the number of servers attacked and their degree of criticality. Regaining control often requires rebuilding solid foundations, and in particular completely reinstalling the Active Directory. From these solid bases, it will be possible to gradually recreate zones of trust by privileging the most sensitive functions within the organization.

Investments linked to these reconstruction plans can be very hefty, often exceeding tens of millions of dollars according to our sources. As such, vigilance must absolutely be maintained in cleaned areas to avoid any further attacks. This requires implementing all the procedures necessary to ensure their security (secured administration, daily log analysis, network filtering, remote access management, etc.).

Medium-term strategy based on anticipation

As of now, it is necessary to overhaul crisis-management processes. Cybercrime scenarios must be included in operating procedures (response procedures, specialised cyber crisis cell, etc.). Relationships with competent authorities must be created or reinforced with the aim to stepping up the mobilisation of these key players.

A coherent communication strategy must be defined in relation to the players involved in and around the organization in question. Organizations should anticipate eventual regulatory constraints (such as client notification in the event of personal-data leaks, etc.). In that case, the crisis will probably go public and that should be anticipated.

Since targeted attacks often comprise a series of individual incidents, it is necessary to simultaneously review incident-management processes to adopt an iterative approach, guaranteeing constant monitoring, rapidity of intervention and a facility to step back and take a wider look at the situation.

> « It is necessary to overhaul the crisis-management process so as to integrate cybercrime scenarios in operating procedures »

In the medium term, by assessing its attractiveness and knowing its key assets, an organization can determine the information that could attract malicious actors and therefore anticipate future attacks. Sector of activity and market positioning are decisive elements. In addition to internal data, relationships maintained with certain partnerships or clients can enhance appeal for hackers (like for a defence contractor or a telecom operator). This assessment should be included in regular risk reviews with the business divisions.

In addition, advanced measures should be implemented to reinforce the security of targets identified in conjunction with the business divisions by isolating the most sensitive perimeters (key business applications, VIP, executive committee etc.) and key technical systems (servers, administration workstation, centralized systems such as the Active Directory). More active approaches, such as requests for closure of sites for exfiltration, and honeypot, etc. may also be envisaged.

Heightening complexity of attacks to diminish returns

Targeted attacks present a challenge for large organizations unaccustomed to managing this type of large-scale, silent crisis which combines business and IT divisions and results in a loss of confidence in the organization's IT System. Managing cyberattacks necessitates reviewing the processes and measures in place, and determining the course of action to be undertaken to complicate the process of carrying out attacks, facilitate their detection and reinforce the organization's reaction capacity.

Implementing these elements will make it more difficult for intruders to strike, and, ultimately, render the attack less profitable! This is clearly one of the keys to successfully addressing these new threats.

WAVESTONE

www.wavestone.com

Wavestone is a consulting firm, created from the merger of Solucom and Kurt Salmon's European Business (excluding retails and consumer goods outside of France).

Wavestone's mission is to enlighten and guide their clients in their most critical decisions, drawing on functional, sectoral and technological expertise.

2016 I © WAVESTONE