Endpoint Protection

symantec.com/connect/blogs/butterfly-profiting-high-level-corporate-attacks

Jul 08, 2015 07:35 AM

A L Johnson

Note: "Morpho" was used in the original publication to refer to this attack group. Symantec has renamed the group "Butterfly" to avoid any link whatsoever to other legitimate corporate entities named "Morpho"

A corporate espionage group has compromised a string of major corporations over the past three years in order to steal confidential information and intellectual property. The gang, which Symantec calls Butterfly, is not-state sponsored, rather financially motivated. It has attacked multi-billion dollar companies operating in the internet, IT software, pharmaceutical, and commodities sectors. Twitter, Facebook, Apple, and Microsoft are among the companies who have publicly acknowledged attacks.

Butterfly is technically proficient and well resourced. The group has developed a suite of custom malware tools capable of attacking both Windows and Apple computers, and appears to have used at least one zero-day vulnerability in its attacks. It keeps a low profile and maintains good operational security. After successfully compromising a target organization, it cleans up after itself before moving on to its next target.

This group operates at a much higher level than the average cybercrime gang. It is not interested in stealing credit card details or customer databases and is instead focused on high-level corporate information. Butterfly may be selling this information to the highest bidder or may be operating as hackers for hire. Stolen information could also be used for insider-trading purposes.

A history of ambitious attacks

The first signs of Butterfly's activities emerged in early 2013 when several major technology and internet firms were compromised. Twitter, Facebook, Apple and Microsoft disclosed that they had been compromised by very similar attacks. The attackers attacked victims by compromising a website used by mobile developers and using a Java zero-day exploit to infect them with malware.

The malware used in these attacks was a Mac OS X back door known as OSX.Pintsized. Subsequent analysis by security researcher Eric Romang identified a Windows back door, Backdoor.Jiripbot, which was also used in the attacks.

Following this flurry of publicity, the Butterfly group slipped back into the shadows. However, an investigation by Symantec has found that the group has been active since at least March 2012 and its attacks have not only continued to the present day, but have also increased in number. Symantec has to date discovered 49 different organizations in more than 20 countries that have been attacked by Butterfly. Over time, a picture has emerged of a cybercrime gang systematically targeting large corporations in order to steal confidential data.

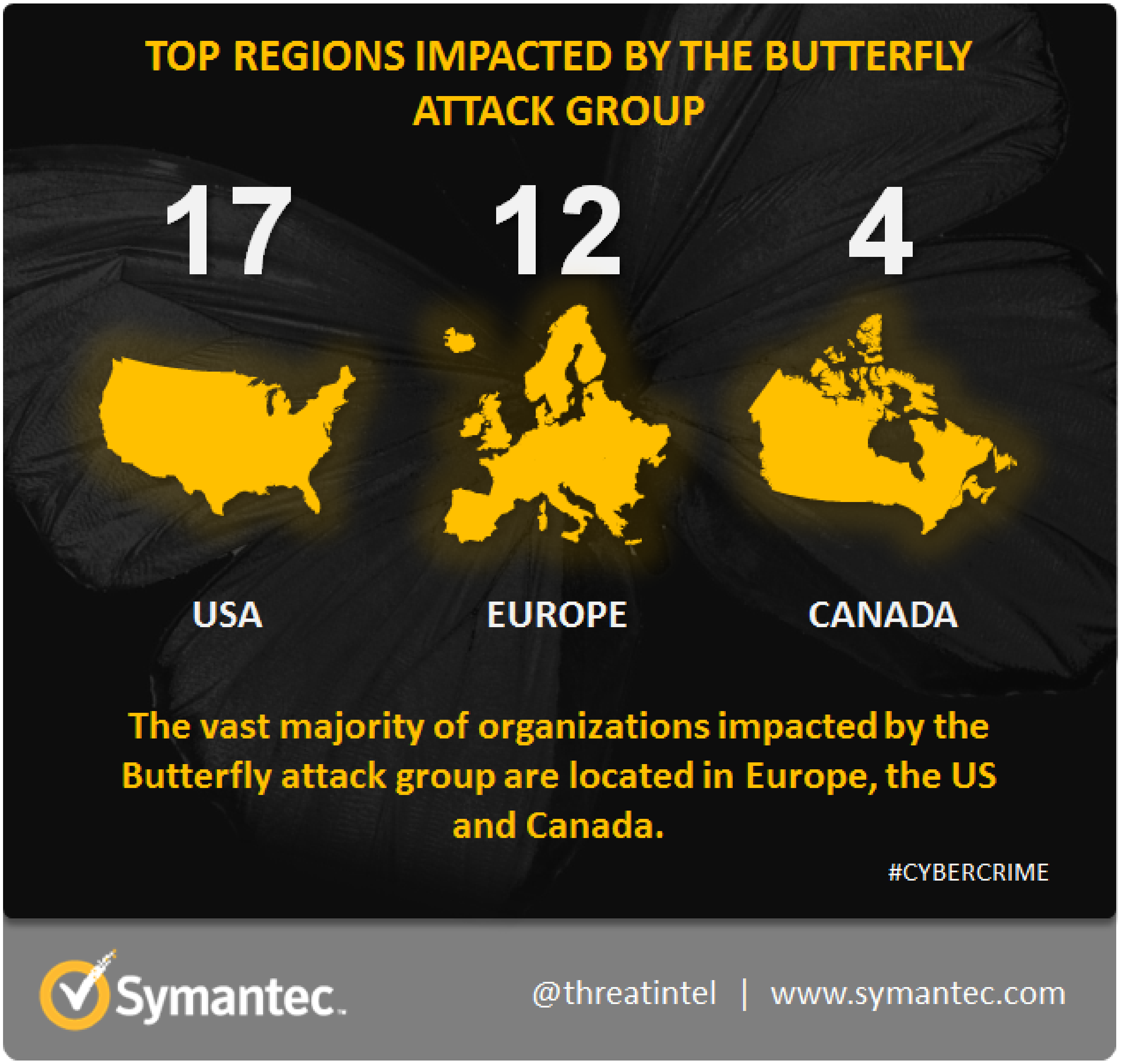
TOP REGIONS IMPACTED BY THE BUTTERFLY ATTACK GROUP
17
12
4
USA
EUROPE
CANADA
The vast majority of organizations impacted by the Butterfly attack group are located in Europe, the US and Canada.
#CYBERCRIME
Symantec.
@threatintel | www.symantec.com

Figure 1. Top regions impacted by the Butterfly attack group

Multiple sectors targeted

Aside from the four companies which have publicly acknowledged attacks, Symantec has identified five other large technology firms compromised by Butterfly, primarily headquartered in the US. However, technology is not the only sector the group has focused on and Symantec has found evidence that Butterfly has attacked three major European pharmaceutical firms. In the first attack, the attackers gained a foothold by first attacking a small European office belonging to one firm and using this infection to then move on to its US office and European headquarters. This template appeared to be followed in the two subsequent attacks on big pharma firms, with Butterfly compromising computers in a number of regional offices before being discovered.

Butterfly has also shown an interest in the commodities sector, attacking two major companies involved in gold and oil in late 2014. In addition to this, the Central Asian offices of a global law firm were compromised in June 2015. The company specializes in finance and natural resources specific to that region. The latter was one of at least three law firms the group has targeted over the past three years.

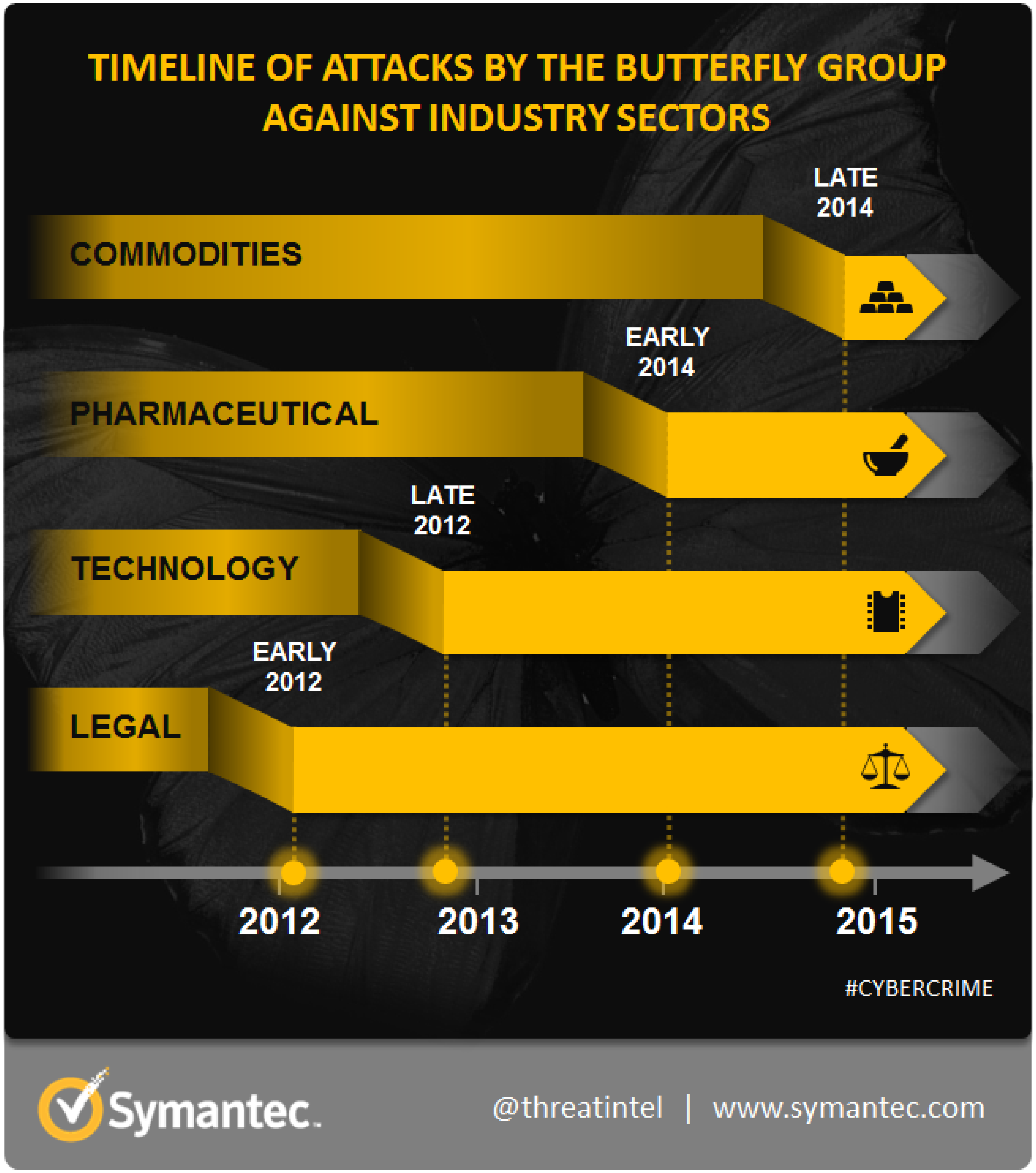

Figure 2. Timeline showing when attacks against different industry sectors began

Stolen information
Butterfly appears to have a good working knowledge of the organizations it is attacking and is focused on stealing specific kinds of information. In many attacks, the group has succeeded in compromising Microsoft Exchange or Lotus Domino email servers in order to intercept company emails and possibly use them to send counterfeit emails.

The group has also attacked enterprise content management systems, which would often be home to legal and policy documents, financial records, product descriptions, and training documents.

In some instances, the group has zoned in on specialist systems. For example, one attack saw it gain access to a Physical Security Information Management (PSIM) system, which is used for managing and monitoring physical security systems, including swipe card access. This could have provided the attackers with access to CCTV feeds, allowing them to track the movement of people around buildings.

Suite of custom malware tools
Butterfly has a number of malware tools at its disposal, all of which appear to be internally developed. Each tool is well documented, indicating that a group rather than an individual is responsible for the attacks.

Its primary tools are two back door Trojans. OSX.Pintsized is capable of opening a back door on Mac OS X computers. Its Windows counterpart is Backdoor.Jiripbot, which has shown signs of continuous development over the past two years, with various minor features being removed or added.

Butterfly has also developed a number of its own hacking tools. Hacktool.Securetunnel is a modified version of OpenSSH which contains additional code to pass a command-and-control (C&C) server address and port to a compromised computer.

Hacktool.Bannerjack is meanwhile used to retrieve default messages issued by Telnet, HTTP, and generic Transmission Control Protocol (TCP) servers. Symantec believes it is used to locate any potentially vulnerable servers on the local network, likely including printers, routers, HTTP servers, and any other generic TCP server. Butterfly uses Hacktool.Multipurpose to help it move across a compromised networking by editing event logs to hide activity, dumping passwords, securely deleting files, encrypting files, and carrying out basic network enumeration.

The group uses Hacktool.Eventlog to parse event logs, dumping out ones of interest, and delete entries. It also kills processes and performs a secure self-delete. Hacktool.Proxy.A is used to create a proxy connection that allows attackers to route traffic through an intermediary node, onto their destination node.

Motivated by financial gain
Based on the profile of the victims and the type of information targeted by the attackers, Symantec believes that Butterfly is financially motivated, stealing information it can potentially profit from. The group appears to be agnostic about the nationality of its targets, leading us to believe that Butterfly is unaffiliated to any nation state.

The group's malware is documented in fluent English, indicating that some of the group members, if not all, can speak the language. They also display some knowledge of English-speaking pop culture, such as using the meme AYBABTU (All your base are belong to us) as an encryption key in Backdoor.Jiripbot.

Command-and-control server activity is highest at times that correspond to the US working day, which may suggest some or all of the group are operating in this region. However, this could also be accounted for by the fact that many of the group's victims are located in the US.

Butterfly may profit from its attacks in a number of ways. The group may be operating as "hackers for hire", targeting corporations on request. Alternatively, it may select its own targets and either sell stolen information to the highest bidder or use it for insider-trading purposes.

Butterfly is a disciplined, technically capable group with a high level of operational security. Having managed to increase its level of activity over the past three years while maintaining a low profile, the group poses a threat that ought to be taken seriously by corporations.

Protection
Symantec and Norton products have the following protections against the Butterfly toolset:

Antivirus

Intrusion prevention system

Further reading
For detailed technical analysis and indicators of compromise, please read our whitepaper: Butterfly: Corporate spies out for financial gain

SECURITY RESPONSE

Butterfly: Corporate spies out for financial gain

Symantec Security Response

Version 1.0 – July 8, 2015

“There are some indications that this group may be made up of native English speakers, are familiar with Western culture, and may operate from an Eastern Standard Time (EST) time zone.”

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr