Cyber Threat Prevention Alert from Bell - July 2018

World governments hit by covert spear phishing attacks

When foreign affairs ministries in Europe and North America received an official-looking email this past February with the subject, "Invitation to a Defense Event," few guessed it contained malware ready to attack their systems and expose potentially sensitive information.

How it works
Attack hidden in Excel macros

Phishing is a cybercrime that tries to trick users into opening malicious links or attachments programmed to steal sensitive information or install malware. Phishing attempts use email spoofing and other techniques to masquerade as official sources, like a bank or retailer.

While traditional phishing attacks cast a wide net, spear phishing is highly targeted. Attackers choose their victims deliberately. They tailor the emails they send to minimize suspicion, often impersonating a person or organization recipients have no reason to distrust.

In the February 2018 attack, the email included an Excel document with a malicious macro. Microsoft Office disables macros by default to protect against these kinds of attacks. This message, however, directed recipients to enable macros if they had trouble viewing the attachment – which they did because the file was programmed to hide certain content. Recipients who followed the direction would see what looked like legitimate listing of upcoming events while the macro fulfilled its purpose in the background.

The macro was set up to unpack and install malware that would give the attackers complete control of the infected system. What made the threat hard to detect was that the executable malware file was bundled with the Excel document. This allowed the malware to install without connecting to an external network source, making it impossible to detect the attack by analyzing network activity for suspicious IPs.

The attacker
Fancy Bear

Fancy Bear is a well-known hacker group believed to be behind these attacks. Classed as an advanced persistent threat (APT) group, it deals in cyberespionage and data theft through spear phishing emails and network-compromising malware – some of which is publicly available and others which have been developed by Fancy Bear to target multiple operating systems.

The group has been active since 2007 and has several known aliases including APT28 and Sofacy.

Bell

The Excel document, before and after activating the macros:

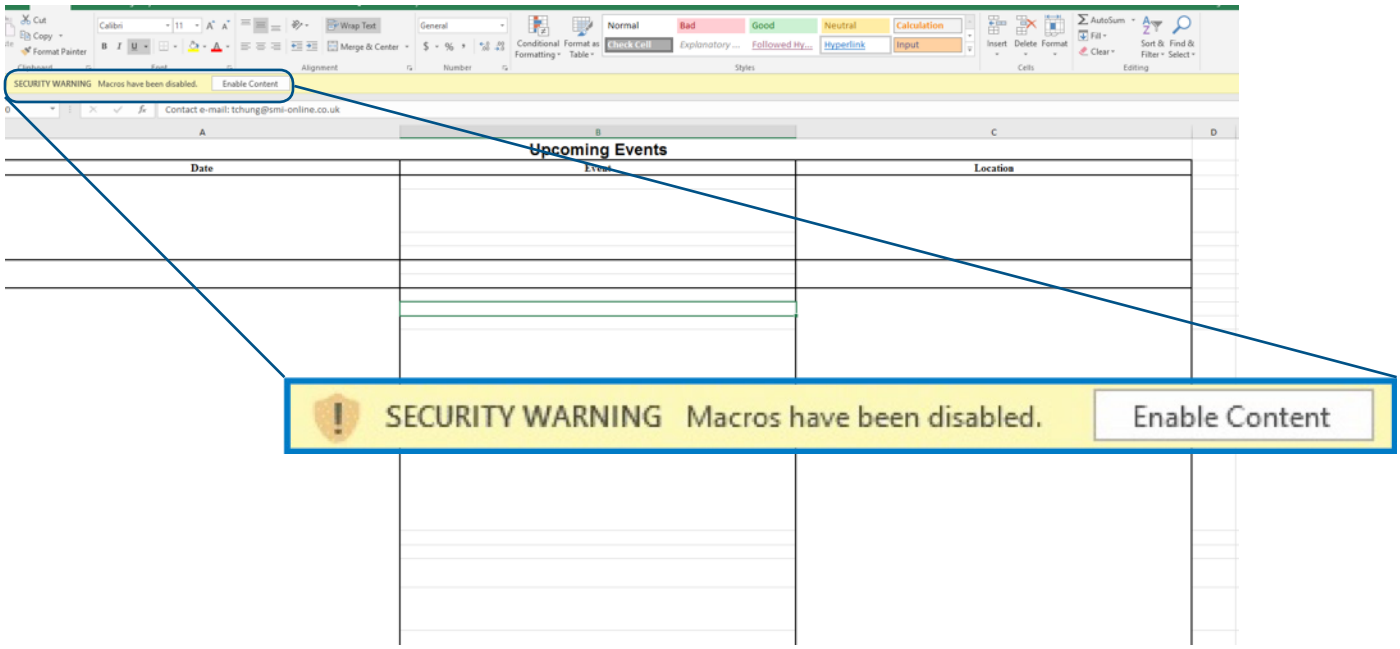


Figure 1. The attachment with macros off — and the prompt to enable them.

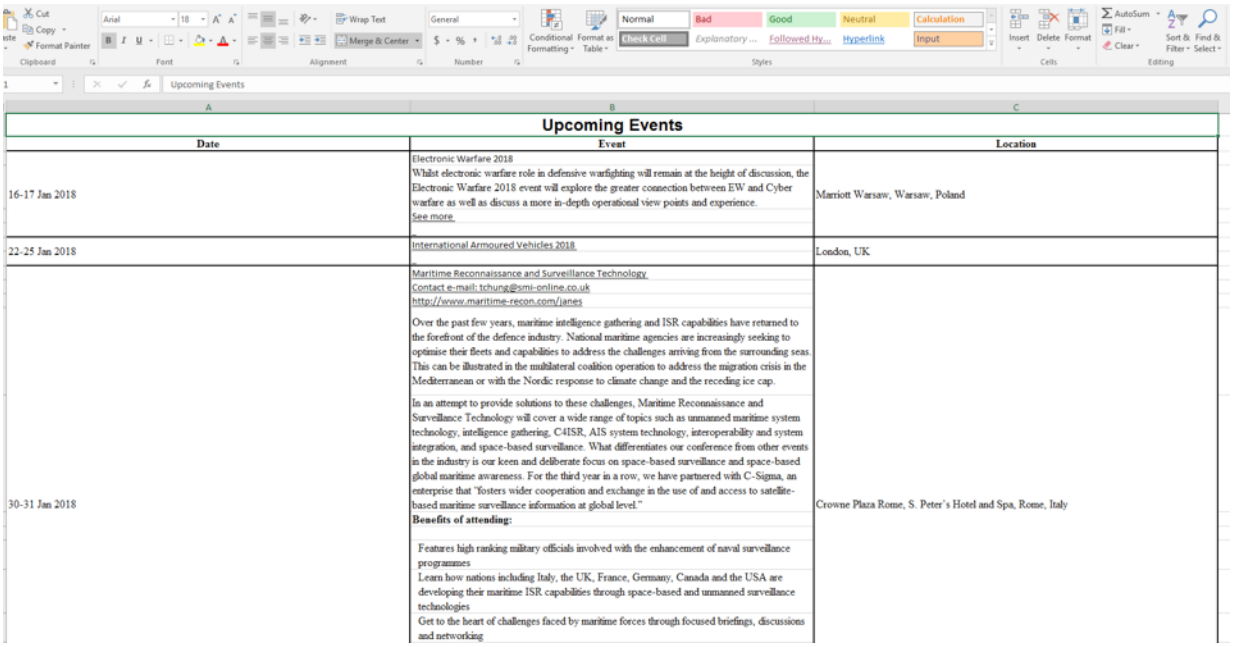


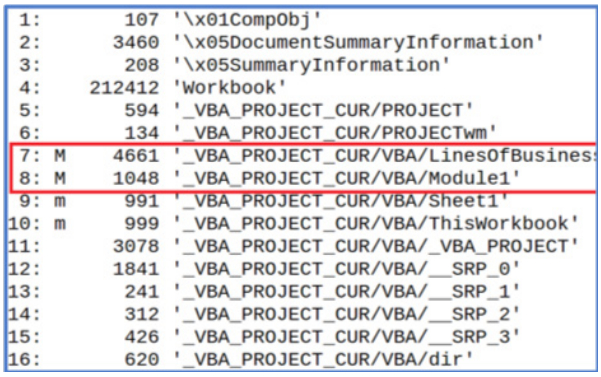
Figure 2: The attachment with macros on.

HOW BELL DETECTED THE THREAT

Extracting the macros to see where they lead

The Bell Cyber Threat Intelligence team continuously monitors the activities of advanced persistent threat groups around the globe to verify if they're active in Canada. When Bell learned this threat was highly active in Canada, our experts analyzed a sample of the file to study its behaviour and determine prevention strategies.

Bell's threat analysis team scanned the Excel document and found two embedded macros. The first was coded to call a function in the second that would install a malicious executable on the recipient's system. Bell found the macro was accessing content hidden from view at the end of the Excel file (at the end of empty rows in the excel document, where victims were unlikely to see it).



```
 1:       107 '\x01CompObj'
 2:      3460 '\x05DocumentSummaryInformation'
 3:       208 '\x05SummaryInformation'
 4:    212412 'Workbook'
 5:       594 '_VBA_PROJECT_CUR/PROJECT'
 6:       134 '_VBA_PROJECT_CUR/PROJECTwm'
 7: M     4661 '_VBA_PROJECT_CUR/VBA/LinesOfBusines
 8: M     1048 '_VBA_PROJECT_CUR/VBA/Module1'
 9: m      991 '_VBA_PROJECT_CUR/VBA/Sheet1'
10: m      999 '_VBA_PROJECT_CUR/VBA/ThisWorkbook'
11:      3078 '_VBA_PROJECT_CUR/VBA/_VBA_PROJECT'
12:      1841 '_VBA_PROJECT_CUR/VBA/__SRP_0'
13:       241 '_VBA_PROJECT_CUR/VBA/__SRP_1'
14:       312 '_VBA_PROJECT_CUR/VBA/__SRP_2'
15:       426 '_VBA_PROJECT_CUR/VBA/__SRP_3'
16:       620 '_VBA_PROJECT_CUR/VBA/dir'
```

Figure 3. Suspicious object embedded in the document

A second macro merged the content of the hidden cells to create .txt and .exe files that gave access to the target computer's file system. The generated executable performed most of the malicious activity – making itself persistent to survive a reboot, connecting to an external IP/domain to send and receive data, and more.

How to prevent these attacks

Network security and employee education are key

Enterprises can protect their users and IT systems from spear phishing attacks like the Fancy Bear attack by:

- Preventing executables from being activated in random places
- Disabling users' ability to enable execution of untrusted macros
- Blocking email attachments from unknown sources with file types that warrant suspicion
- Scanning attachments with multiple antivirus engines and sandbox technologies
- Training and educating employees on how to properly handle suspicious emails

Along with these measures, a periodic security assessment or organizational health check can help identify IT security gaps and focus remediation on the most important areas.

Want to make sure your enterprise is protected against cyber threats like these?
Visit Bell.ca/cyberdefence to learn more on how we can assist you.

Bell