NTT Security

GTIC Monthly Threat Report

July 2018

Contents

2018 FIFA World Cup Increase in Cyber Activity

Lead Analyst: Aaron Perkins

It is no secret that international events draw the attention of would-be cyber attackers, and the recent 2018 FIFA World Cup, the international football (soccer) championship, was no exception.

Russia claimed to have thwarted over 25 million cyber attacks, though security researchers around the globe continue to question that number.

The NTT Security Global Threat Intelligence Center (GTIC) also gathered information concerning actual attacks during, and leading up to, the World Cup. What GTIC researchers found was the majority of the attacks with a World Cup theme were phishing emails, attempting to trick users into opening malicious documents.

GTIC researcher, Terrance DeJesus, notes that malicious file types were mostly .pdf (Adobe) at 51 percent, followed by .doc (Microsoft Word documents) at 31 percent, .xlsx (Microsoft Excel files) at 11 percent, and .rtf (Rich Text Format) at four percent, with other file types rounding out the remaining three percent.

The security community also discovered a World-Cup-themed attack campaign targeting Android users. NTT Security partner, Symantec, noted that this Android-focused campaign appeared to be hurriedly created, targeting Israeli citizens and military personnel.

Large sporting events take place regularly, and the 2018 FIFA World Cup is just a single example of attackers leveraging consumers' thirst for information concerning the event to socially engineer the unwitting victim into downloading malicious files, visiting infected websites, or installing malicious mobile applications.

No matter who you're cheering for during the next big sports event, it is critical to remain vigilant and understand that the increased interest in the event also increases risk for individuals, as well as enterprises.

References:

Russia reports stopping 25 million cyber attacks

Attackers targeting World Cup fans with Android spyware

Collaboration Tools: The Latest Threat from the Inside(r)

Lead Analyst: Danika Blessman

Enhanced productivity. Better communication with other teams. Seamless coordination.

All are benefits to using collaboration tools, but has your organization considered these applications may be leveraged as an attack vector from an insider threat?

Tools like Skype, Yammer, and Smartsheet – just to name a few – provide incredible ease with which one can share documents and communicate with teammates. These tools may seem innocuous but could become a means for losing sensitive data, like personally identifiable information or proprietary company plans, if misused by the unwitting – or intentional – insider.

These tools may feel like a casual form of communication among employees, clients or outside organizations. They can potentially result in users letting their guard down and giving out information they wouldn't disclose in a more formal channel. Or they could be a means for inappropriate communication, which could in turn hurt an organization's reputation.

Like the insider threat itself, these types of threats are nothing new; collaboration tools simply provide one more means – a very effective one, at that – of leaking sensitive or proprietary information.

The insider threat is not going away, nor is the use of collaboration tools. In fact, the 2018 NTT Security Risk: Value Report states that, although not always malicious in nature, the insider threat is an organization's most significant weakness. Another recent report reveals 57 percent of organizations will increase spending on collaborative tools this year, suggesting an increase in usage as a result.

Another recent study of more than one million employee messages revealed some surprising results. One in every 118 public communications included confidential information, and one in every 262 public messages included passwords.

Worse yet, via private messaging channels, one in 149 messages contained passwords, and one in 190 messages contained confidential data.

Even well-meaning employees make mistakes – or have lapses in judgment – in the name of good communication or customer service; it's human nature to want to help. Unfortunately, this increases the risk of social engineering through these collaborative tools – including clicking on malicious links shared via collaboration tools or disclosing sensitive data.

This doesn't suggest that these tools should be eliminated from the workspace – they are essential in today's environment. Organizations simply need to be aware of the risks and train users in safe(r) use.

There are, however, steps that can be taken to mitigate your organization's risk from insider threats:

- Have a written, established incident response plan in place.
- If it does not impact your operations, consider implementing a solution that makes it more difficult to send attachments outside the organization.
- Implement "protecting information security" into each employee's goals and objectives.
- Conduct a thorough risk assessment to determine what your most valuable information is and who should have access to that information.

References:
Insider Dangers Are Hiding in Collaboration Tools
Human Behavior Risk Analysis
NTT Security Risk:Value Report

Cisco Notifies Clients of Remote Code Execution Vulnerability

Lead Analyst: Jose Hernandez

Cisco FXOS and NXOS Fabric Services Remote Code Execution Vulnerability

Threat Status: High

CVE-2018-0304

Severity: **Critical** (CVSS: 9.8)

Date: 12 July 2018

Remediation Details: Cisco has released software patches to address this vulnerability.

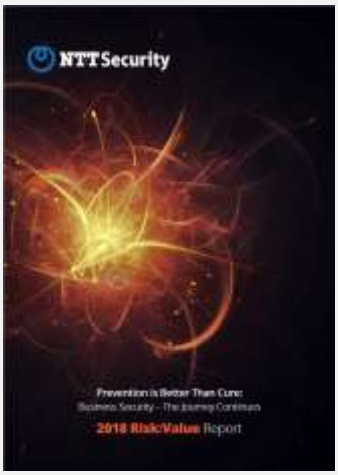
Affected Versions:

- Firepower 4100 Series Next-Generation Firewalls
- Firepower 9300 Security Appliance
- MDS 9000 Series Multilayer Switches
- Nexus 2000 Series Fabric Extenders
- Nexus 3000 Series Switches
- Nexus 3500 Platform Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode

- Nexus 9500 R-Series Line Cards and Fabric Modules
- UCS 6100 Series Fabric Interconnects
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects

Analyst Note: Cisco discovered a critical vulnerability in the Fabric Services component of the NXOS and FXOS software. Cisco Fabric Service allows network administrators to distribute and synchronize configuration data of Cisco devices on the same network. The vulnerability lies in the failure to validate Cisco Fabric Service packet headers. An attacker can exploit this vulnerability by sending a specially crafted packet to an affected device. The vulnerability allows an unauthenticated attacker the ability to execute arbitrary code with root privileges, read sensitive memory, and cause a denial of service condition. While there are no workarounds to address this issue beyond the patch Cisco released, the attack vector can be reduced by limiting the distribution types used by Cisco Fabric Services.

NTT Security Annual Reports



Risk:Value 2018

Many organizations are stuck in a reactive mindset when it comes to information security and would opt to pay a hacker's ransom rather than proactively invest in security. That's a key finding in this year's Risk:Value 2018 Report.

Download your copy today!

2018 Global Threat Intelligence Report

This year's report summarizes activity we detected in over 6.1 trillion+ logs and more than 150 million+ attacks, along with vulnerability scans, incident response engagements, and diverse findings from threat research and threat intelligence teams across NTT Security.

Download your copy today!

About GTIC

The NTT Security GTIC protects and informs NTT Group clients through security threat research, vulnerability analysis and the development of effective countermeasures. For more information, including vulnerability disclosures, threat reports and white papers, visit the resource page on www.nttsecurity.com or our blog.