McAfee LLC
2821 Mission College Blvd.
Santa Clara, CA 95054-1549

Updated: 04.20.17

McAfee Strategic Intelligence/Shamoon 2

Announcement Q&A

1. What is the news?

- **McAfee has linked a series of cyber-attacks in Saudi Arabia to a common malicious actor rather than to individual cyber gangs in the region.** McAfee Strategic Intelligence researchers have released evidence that a series of cyber-attacks targeting the Persian Gulf and, specifically, Saudia Arabia between 2012 and the present are the work of hacker groups supported and coordinated by a common malicious actor, and not the random efforts of a variety of individual cyber gangs in the region.

- **The latest Shamoon campaigns go beyond a few targets in energy, to many in other critical sectors that run Saudi Arabia.** Whereas earlier Shamoon campaigns targeted a relatively small number of energy sector organizations to disrupt the operations of the region's critical industry, the new attacks are focused on a greater number of organizations in the energy, government, financial services and critical infrastructure sectors of Saudi Arabia to disrupt that entire country.

- **The large-scale, sophisticated, coordinated nature of the latest campaigns suggest the activity of a nation-state actor.** Taken together, this new series of Shamoon cyber espionage campaigns are significantly larger, well-planned, well-resourced, and coordinated at a level beyond the limited capacity of disparate independent hacker gangs.

2. How can McAfee make these claims?

- McAfee Strategic Intelligence surveyed the evolution of Shamoon-based attacks, from the 2012 attacks on the Persian Gulf energy sector, to the latest campaigns in Saudia Arabia in 2016 and 2017.
- McAfee found commonalities between the Shamoon malware samples, tactics and even infrastructure used in these attacks:

    - The new attacks used 90% of the original code from the 2012 attacks
    - The macro code used in the latest spear-phishing campaign was also used in the attacks launched by Rocket Kitten in Spring 2016
    - Some of the new attacks also used some of the same infrastructure previously used by the Oil-RIG campaign in late 2015.

-- more --

3. Why is this different from previous Shamoon discoveries and revelations?

- Past research has examined Shamoon attacks in depth, but haven't brought forward evidence of a substantial overlap in code, tactics and infrastructure to the extent McAfee has today.

4. How do these attacks work?

- **Step 1.** Once a target is identified, the attackers send spear-phishing emails to individuals working within the organization. The recipients of these messages are chosen carefully, with the assumption that they will enable network access to the most sensitive information and systems in the organization.
- **Step 2.** The email recipient is lured into clicking on a link within the email or opening a Microsoft Office file embedded with macros that allow the attackers to create backdoor access to the organizations.
- **Step 3.** The attackers conduct reconnaissance across the network to identify valuable information and critical systems.
- **Step 4.** Once the reconnaissance is complete, the attackers weaponize the attack and wipe the hard drives of the master boot records (MBRs). In the 2016 to present case, the attackers launched multiple simultaneous waves of attacks:
    - **Attack Wave 1:** Wiped systems on November 17, 2016, at 20:45 Saudi time.
    - **Attack Wave 2:** Wiped systems on November 29, 2016, at 01:30 Saudi time.
    - **Attack Wave 3:** Began January 23, 2017, and ongoing, with similar samples and methods and TTPs as in Waves 1 and 2.

5. What was the impact of these attacks?

- In 2012, the actors moved quickly in and out of the victim's network, inflicting system-wipe damage and then disappearing.
- In 2016, the actors penetrated networks and established remote control to gather intelligence for future planned wiping attacks.
- Unless thwarted, the attackers could have exfiltrated any data of value to them, and then erased the systems' data and made them unable to boot up and operate.

6. What does this discovery mean?

- These findings are the latest evidence of rogue state or stateless actors developing increasingly sophisticated and powerful cyberwarfare and cyber espionage capabilities to project geopolitical and strategic power that would otherwise be beyond their reach.
- Such actors may seek to acquire cyber capabilities from the Black Market in the same way North Korea looked to Pakistan's Abdul Qadeer Khan to acquire nuclear technologies.
- They may choose to collaborate with other aspiring actors as Iran and North Korea have in the development of ballistic missiles.
- What we know for certain is that cyber tools, tactics, knowledge, talent and infrastructure are similarly available to actors wishing to acquire them.

7. What else did McAfee announce today?

- McAfee announced the formation of McAfee Strategic Intelligence, a new research team charged with investigating the technology and tactics of the latest cyberwarfare and cybercrime campaigns, and working with law enforcement to take action against networks of cybercriminals.
- The creation of Strategic Intelligence firmly establishes McAfee's commitment to understanding the cyber threat landscape, and will complement the work of McAfee Labs, one of the world's most prominent sources of threat intelligence data, and the technology vulnerability research conducted by the Advanced Threat Research team.

8. What is McAfee Strategic Intelligence's mission?

- **The McAfee Strategic Intelligence team** will investigate the latest threats, their design, and how they are built into cyber-attack campaigns, and inform McAfee customers on how they can protect themselves and learn from these attacks moving forward.
- **Areas of research** will include advanced malware, ransomware, financial fraud, general cybercrime, cyber espionage, cyberwarfare, and protection of industrial control systems.
- **Engagement:** The group will also be the primary vehicle within McAfee for engagement with law enforcement, academia, and other organizations, including efforts to take down criminal networks, develop new approaches to fighting cybercrime, and recruit more young people to join the ranks of cybersecurity professionals.

9. How does McAfee Labs' research charter and mission differ from that of Strategic Intelligence?

- McAfee Labs gathers threat intelligence data from millions of sensors across key threats vectors—file, web, and network—delivers real-time threat intelligence, critical analysis, and expert thinking to improve system protection and reduce risks.
- McAfee Labs develops core threat detection technologies that are incorporated into the broadest security product portfolio in the industry.
- McAfee Labs also engages with McAfee's many cyber threat intelligence sharing partners, including the Cyber Threat Alliance, an independent industry organization committed to facilitating the exchange of the latest threat data. Cyber Threat Alliance partners include Check Point, Cisco, Fortinet, Palo Alto Networks, and Symantec.

10. How does McAfee Advanced Threat Research's charter and mission differ from that of Strategic Intelligence?

- McAfee's Advanced Threat Research group conducts research into vulnerabilities within the foundational hardware and software technologies of the industry.
- Increasingly, people around the world depend on technology for their daily affairs. Making this technology trustworthy requires a deep understanding of how attacks work.

- By researching security vulnerabilities in the areas of hardware, firmware, virtualization technologies and crypto software, the McAfee Advanced Threat Research team plays an important role within McAfee, particularly as connected environments because more diverse.
- Upon discovery of vulnerabilities, the team coordinates the responsible disclosure and timely mitigations with affected technology vendors.