Russian Cyber Espionage Campaign - *Sandworm* Team

Microsoft Windows Zero-day – Targeting NATO, EU, Telecom and Energy Sectors

CVE – 2014-4114

An iSIGHT Partners Overview
Key Points – *Sandworm* Campaign

- **Cyber Espionage Campaign attributed to Russia**
  - Targeting includes
    - NATO
    - Ukraine
    - Poland
    - European Union
    - European Telecommunications
    - Energy Sector
  - Attribution to one of 5 active Russian intrusion teams monitored by iSIGHT Partners
  - “Sandworm Team”
    - Named for its affinity for/coded references to science fiction series *Dune*
    - Campaign partially detailed by researchers at F-Secure and ESET – captured only a small component of targeting and missed critical elements

- **Utilizing Zero-day flaw in Microsoft Windows (CVE-2014-4114)**
  - Spear-phishing campaign using weaponized Microsoft Office documents
    - Visibility into multiple PowerPoint lures
  - Impacts all versions of Windows from Vista to 8.1
    - Flaw has existed for years
  - Zero-day nature of vulnerability leads to conclusion that intrusion efforts were highly effective
  - Close collaboration between iSIGHT Partners and Microsoft - patch is being released on Tuesday, October 14th
Sandworm Campaign - Timeline of Events

- Monitoring Sandworm Team from late 2013 and throughout 2014
  - Genesis of team dates to as early as 2009
  - Increased activity throughout 2014

- Visibility into this specific campaign began in December of 2013
  - NATO alliance targeted as early as December 2013
  - GlobeSec attendees targeted in May 2014
  - June 2014
    - Western European government agency
    - Polish energy firm targeted using CVE-2013-3906
    - BlackEnergy variant configured with Base64-encoded reference to French telecommunications firm
  - Zero-day artifacts captured late August/early September (CVE-2014-4114)
    - Spear-phishing email and exploit targeting Ukrainian government
    - Coinciding with NATO summit on Ukraine in Wales
    - At least one US organization fell victim – think tank/academia

- iSIGHT Partners labs team discovered use of zero-day vulnerability on September 3, 2014

- Immediately notified targeted parties, clients across multiple government and private sector domains

- Began working with Microsoft on September 5, 2014
  - Provided technical analysis of vulnerability and the malware used to exploit it
  - Coordinated tracking of campaign
    - Monitoring for broader targeting and victimization
    - Monitoring for broader use of zero-day exploit in the wild

- Purposely timing disclosure to coincide with the release of the patch
  - Minimizes potential for copy-cat exploit creation
  - Limits exposure to a broad reaching, severe vulnerability
Genesis of Sandworm Team dates to as early as 2009

Late 2013 and throughout 2014
- Monitoring of SandWorm Team
- Traced to 2009
- Increased activity throughout 2014

May 2014
- GlobeSec attendees targeted

June 2014
- Western European government agency
- Polish energy firm targeted (CVE-2013-3906)
- BlackEnergy variant w/Base64-encoded reference to French telecomm firm

September 2014
- Zero-day artifacts captured (CVE-2014-4114)
- Spear-phishing email/exploit targeting Ukrainian government
- Coinciding with NATO summit on Ukraine in Wales
- At least one US org fell victim (think tank/academia)

September 3, 2014
- iSIGHT Partners labs discovers zero-day vulnerability
- Immediately notified targeted parties and clients across government and private sector domains

September 5, 2014
- Began working with Microsoft
- Provided technical analysis of vulnerability and malware used in exploit
- Coordinated tracking of campaign
  - Monitoring for broader targeting and victimization
  - Monitoring for broader use of zero-day exploit in the wild

Purposefully timed disclosure to coincide w/MSFT patch release
- Minimizes potential for copy-cat exploit creation
- Limits exposure to a broad reaching, severe vulnerability
Sandworm Campaign - Visible Targets

Known Targets
- Government
- Academic
- NATO
- Energy
- Telecom
As has become a tradition, GLOBSEC will again try to push higher and farther with the 2014 edition of what has become the largest security and policy forum in Central Europe.

The ninth annual GLOBSEC Forum, scheduled to take place between 14-16 May in Bratislava, Slovakia, will explore, among other foreign policy and security issues, changes in the 21st century power balance, ability and political will of NATO member states to intervene and the consequences of the latest Syria bombings.

GLOBSEC has grown into what US veteran analyst dagmar Breseman calls a “global operation”, annually attracting over 100 participants from more than 90 countries.

GLOBSEC 2014 will feature the highest ministerial presence of any Central European conference. Among the confirmed guests are Prime Minister Mateusz Morawiecki, his Hungarian counterpart Viktor Orbán, along with foreign ministers of Slovakia, Hungary and Norway. On a trans-governmental level, Lord Fras, former British Defence Secretary, UN Special Representative for Afghanistan Ali Rahbi, and Michael Chertoff, former US Secretary of Homeland Security are scheduled to participate.

Spear-phishing attachment

GlobeSec Forum on Russia

Diplomacy spear-phishing attachment

A recent Wood Mackenzie report predicts that shale gas will account for 30% of the US market by 2020. Oil and industry experts, such as T. Boone Pickens, are even optimistic and predict that shale gas will account for over 50% of the US market. Even at the low estimate of 30%, shale gas will have a major impact on the industry and the production of gas. The new reality is that the conventional reserves of natural gas, the Middle East and Russia are receding, leading to some gas and no living matter. Shale projects have contributed a deep U.S. gas price from $3.89 per million British thermal units in 2008 to an average of about $4.45 in 2014. Gasprices have doubled, developing the massive Bakken Shale gas (e.g. US) and now the shale gas, which has several US demand for foreign gas.

Energy spear-phishing attachment, specifically crafted for Polish audience

Zero-day spear-phishing attachment, purported list of Russian sympathizers/“terrorist” actors

Diplomatic Failow. Europe’s Struggle for Strategic Competitiveness

The crisis in Ukraine, most often portrayed with its economic problems over the past few years, escalated with two strange challenges last week. The first involved a trip to Kiev by Russia over Ukraine. The second involved in Geneva, where the UN’s foreign policy chief Catherine Ashton, chased took in Iran’s nuclear program. The EU agreed to the first, but in Ukraine President Vladimir Putin’s involvement has been an agreement opposed to the same under pressure from Moscow. By contrast, the Geneva negotiations remained on waiting notice, as Ukraine agreed to temporarily relax its economic restrictions in exchange for mild sanctions relief while the EU demanded a comprehensive deal that was U.S. Secretary of State John Kerry called Russia’s “bureaucracy” of the process.

The two episodes involved the European foreign policy debates often lack emotion. Discussions of Iran and the world frequently revolve around good intentions of principles and international influence. The stakes in Ukraine and Iran are real and significant. Ukraine has become a trial of the EU’s ability to manage its strategic neighborhood and any Russia from managing control over former Soviet states. Iran has tested Europe’s patience to projetoepicurean in the middle power.

The EU has long aimed to be both a regional and global power. The nation’s leaders articulated these goals in the eight—what is now—European Union strategy in 2000. Developed by Adams’s predecessor, Joschka Fischer, it sought to make the EU a European way of life, for energy, for the strategy presented “building a new democratic and political community.” The document will reach its 10th birthday this December. Is it fit for the purpose?

At the national level, the EU faced a recession lasting 16 years. It grew at the rates of a major
Marked increase in cyber espionage activities linked to Russia
- Russia is increasing its cyber-espionage focus and the volume is up in 2014
- iSIGHT recently detailed activities of Tsar Team
  - Mobile malware targeting multiple platforms
    - Android, Windows, iOS
  - Targets include
    - Foreign militaries
    - Defense contractors
    - Ministries of foreign affairs
    - News organizations
    - NGOs and multilaterals
    - Jihadists

Sandworm is one of 5 active cyber intrusion teams linked to Russia being monitored by iSIGHT Partners
- Activities date back as far as 2009
- Identified through overlapping infrastructure, use of traditional crimeware, unique references to Dune
- Team has an affinity for using traditional cyber crime tools as a component of its activities
  - BlackEnergy malware
    - Used at least 2 versions of BlackEnergy
      - BlackEnergy 2 – traditional crimeware
      - BlackEnergy 3 (Lite)
        - No documented use in crime – may have been purpose built for Sandworm
    - Samples tied on basis of configuration to same combination of internal proxies
      - Up to 7 proxies in common

iSIGHT Partners believes Sandworm Team has Russian origins based on several factors:
1. Files retrieved from an open directory on a command and control server included a directory listing in Russian and a help file for the BlackEnergy Trojan also written in Russian
2. Known targeting is consistent with antagonists to NATO as well as Ukrainian and European Union governments.
3. Social engineering is designed to appeal to personnel involved in military and intelligence operations against Russia such as a list of pro-Russian “terrorists” sent in an email.
4. BlackEnergy source code was released through Russian e-crime channels.

List of Purported pro-Russian "Terrorists"
Growing trend of blurred lines across cyber threat domains
- Not just in Russia but more pronounced here recently

Russian overlap
- Links between criminal activity and cyber espionage activity is not uncommon
  - Tools
  - Talent
- Some examples...
  - Zeus used in massive espionage campaign against US Government in 2008 and again in 2012
  - Pro-Russian hacktivism used BlackEnergy in the past during Georgian conflict
  - Russians allegedly contracted a cyber crime actor in Georbot campaign against Georgia
    - Attributed to Eshkinkot – Russian national named Vladimir A. Lenskij
    - Georgie CERT claimed to have captured e-mail messages and docs from Russian handlers
      - Instructing on how to use malware to record audio
      - Capture screen shots
      - Exfiltrate data
  - TEMP.Noble (another Russian intrusion actor monitored by iSIGHT)
    - Sensitive source indicates that malware components were developed through for hire cyber crime forum
- BlackEnergy
  - Criminal actors
  - Sandworm Team
Details - Microsoft Windows Zero Day
CVE – 2014 – 4114

- Affects all supported versions of Microsoft Windows
  - Windows Vista x64 Service Pack 2
  - Windows Vista Service Pack 2
  - Windows Server 2008 R2 x6 Service pack 1
  - Windows Server 2008 Services Pack 2
  - Windows Server 2008 x64 Service Pack 2
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows 7 Service pack 1
  - Windows 7 x64 Service Pack 1
  - Windows 8 x64
  - Windows 8
  - Windows 8.1 x64
  - Windows 8.1
  - Windows RT
  - Windows RT 8.1

- Does not appear to affect Windows XP

- Exposed, dangerous method vulnerability
  - OLE package manager in Microsoft Windows and Server
  - Vulnerability allows an attacker to remotely execute arbitrary code
  - Windows allows OLE packager (packager .dll) to download and execute INF files
  - In case of observed exploit, specifically when handling Microsoft PowerPoint files:
    - Packager allows a Package OLE object to reference arbitrary external files (such as INF) from untrusted sources
    - Causes referenced files to be downloaded and executed with specific commands
    - Attacker can exploit to execute arbitrary code
    - Needs specifically crafted file and social engineering methods to convince user to open
Collaboration with Microsoft

- iSIGHT Partners follows Responsible disclosure procedures
  - Targeted entities
  - Government and Law Enforcement
  - Impacted Software vendor(s)
    - Microsoft

- Disclosed identification of zero-day 2 days after analysis
  - Began immediate collaboration with Microsoft
    - Supporting development of a patch
    - Tracking utilization of the vulnerability in the wild

- Timed disclosure to minimize the potential for broader victimization
  - Patch ready for release Tuesday, October 14th
  - “Break in case of emergency” plan in place for past 5 weeks
    - Trigger: Broader propagation of malware targeting vulnerability
    - Trigger: Evidence of broader victimization

- Disable the WebClient Service
  - Impact
    - Web Distributed Authoring and Versioning (WebDAV) requests are not transmitted
    - Any service depending on Web Client service will not start

- Block TCP ports 139 and 445
  - Impact
    - Ports 139 and 445 are used for additional services including Common Internet File System (CIFS), DNS Administration, NetBT service sessions, printer sharing sessions and more
    - Disabling could affect functionality of those services

- Block launching of Executables via Setup Information Files
  - Impact
    - Applications that rely on the use of .INF file to execute an installer application may not automatically execute