



Federal Bureau
of Investigation



US-CERT
United States Computer
Emergency Readiness Team

Public Service Announcement

The Professional Social Network Risk Posed by Advanced Persistent Threat Actors

30 March 2012

The FBI judges that advanced persistent threat (APT) actors have and likely will continue to exploit social networking sites for victim targeting and to facilitate computer network exploitation (CNE). The Robin Sage Experiment presented at Black Hat in 2010 outlines a plausible and proven scenario for APT actors to exploit the connection-driven state of social networking.

In the Robin Sage Experiment, white hat hacker Thomas Ryan created a false persona on Facebook and successfully connected to government and private sector cyber security personnel, eliciting a wealth of information and employment interest. Based on the success of this experiment, the FBI believes professional social networking sitesⁱ—such as LinkedInⁱⁱ—pose even greater operational opportunities for APT actors to target US Government, cleared defense contractor, and private sector personnel. These sites are designed with a professional theme as compared to more typical social networking sites aimed at personal information. Professional networking sites are designed to capture and display work-related information, which can provide good open source opportunities for APT actors to target individuals based on association with an industry sector, company, or projects. Additionally, the professional nature of such sites can mask collection threats as benign communication which may make probes into company information or employment opportunities seem more legitimate than contact on personal social networking sites.

The Robin Sage Experiment

In December 2009, white hat hacker Thomas Ryan created a false identity on Facebook as a 28-day experiment. The experiment included creation of a false persona of a young female thought to be attractive and edgy in appearance who identified herself as a “cyber threat analyst” at Naval Network Warfare Command. Through the 28 days, Thomas Ryan attempted to connect with as many cyber security and government personnel as he could to garner information sharing and see what opportunities might become available. The experiment was successful in quickly propagating new connections based on mutual connectedness. The findings were reported in a paper and presentation titled “Getting In Bed With Robin Sage” at the Black Hat conference in Las Vegas in 2010.

ⁱ Professional Social Networking sites are designed to manage professional (personal or corporate) identities in a social environment by building and engaging connections.

ⁱⁱ LinkedIn is the most popular professional networking site, containing over 150 million members.

A Possible Scenario

An APT actor assuming a false persona could easily connect to companies and persons on LinkedIn related to an industry of interest. Then these connections could drive additional victims into assuming validity of the false identity. Coupling these items could lure people into believing communication with the false identity is benign and legitimate. With a rapport established, the victims might be led to divulge sensitive information or unwittingly aid in facilitating CNE. The APT actor(s) could easily attach either a malicious file purporting to be a seemingly benign attachment, such as a resume, or embed malicious code directly into an attachment which seemingly behaves in a legitimate manner.

APTs versus Hackers/Cyber Criminals

Advanced persistent threat actors differ from common hackers or cyber criminals by conducting targeted, rather than opportunistic, attacks that seek precise information rather than monetary gain, more closely resembling espionage. While the activity cannot often be definitively linked to any particular nation state, the sophistication, resources, and types of information sought suggests governmental support. APTs have been linked to several high-profile recent cyber attacks including *Operation Aurora* and *Night Dragon*, and the 2007 and 2008 Russian attacks on Estonia and Georgia.^{i,ii}

US-CERT Recommended Mitigation Strategies

To mitigate the threat of APT activity, the United States Computer Emergency Readiness Team (US-CERT) recommends the following actions:

- Audit what information must reside on the network and remove—air gap—vital information from networked devices to ensure data protection.
- Monitor for and report suspicious activity—namely spear phishing messages—especially with a nexus to significant events, meetings, conferences, etc. Corporate e-mail clients might be configurable to checking for phishing messages; however, full reliance on automated systems will likely fail to catch all APT activity.
- Monitor and record network activity levels to more easily identify patterns, trends, and anomalies.
- Follow standard best practices for network security, such as keeping up with patches and virus signatures to prevent known vulnerabilities, restricting administrator level privileges on standard user machines, ensuring passwords are strong and changed on a regular basis, and unused accounts are disabled and promptly removed upon an employee leaving the organization.

- Keep current on information published in US-CERT Early Warning and Indicator Notes (EWINs) and Situational Awareness Reports (SARs).
- Educate users that clicking links on pages or in e-mail may not direct them to where the link URL appears to point to. Hovering the cursor over a link can often reveal the actual URL and manually typing in URLs, rather than clicking links, can often prevent malicious redirect attempts.
- Always treat unsolicited or unexpected e-mails which contain links or attachments and/or probe for sensitive information with the utmost caution, especially those related to significant events, meetings, conferences, etc.
- Educate users about the dangers of social engineering and e-mail phishing, particularly when related to significant events, meetings, conferences, etc.
- Avoid suspicious third-party applications that are promoted by social networking services and educate users that such applications can contain malicious code and unwittingly grant access to otherwise restricted data.
- Additionally, educate users on the dangers of APTs and social networking. Even though social networking sites may be of personal use, APT actors could still target individuals through the use of these sites, which can lead to compromises of corporate networks.
- Regularly evaluate privacy policies to ensure selections are still appropriate, even if the services have changed.

Additional References:

- “Staying Safe on Social Networking Sites” – <http://www.us-cert.gov/cas/tips/ST06-003.html>
- “Social Networking and Security Risks” – http://www.gfi.com/whitepapers/Social_Networking_and_Security_Risks.pdf

Reporting Notice

The FBI and US-CERT encourage recipients of this document to report information concerning suspicious or criminal activity to the local FBI field office. The FBI's 24/7 Strategic Information and Operations Center can be reached by telephone at 202-323-3300 or by e-mail at SIOC@ic.fbi.gov. US-CERT can be reached by telephone at 888-282-0870 or by e-mail at SOC@us-cert.gov. FBI regional phone numbers can be found online at <http://www.fbi.gov/contact/fo/fo.htm>. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. The US-CERT homepage can be found online at www.us-cert.gov.

(U) For comments or questions related to the content or dissemination of this document, please contact the FBI Cyber Intelligence Section, Global National Security Cyber Intelligence Unit (GNSCIU) at 703-961-7611, or the US-CERT at the above-mentioned phone number and e-mail address.

(U) Appendix A: List of Popular Professional Social Networks (in no particular order):

1. LinkedIn
2. Ecademy
3. Focus
4. YorZ
5. Xing
6. Facebook (can be used for professional purposes)
7. Care2
8. Gather
9. MEETin.org
10. Tribe
11. Ziggs
12. Plaxo
13. NetParty
14. Networking for Professionals
15. Biznik
16. Cmypitch.com
17. Cofoundr
18. E.factor
19. Entrepreneur Connect
20. Fast Pitch
21. JASEzone
22. PartnetUp
23. PerfectBusiness
24. Ryze
25. StartupNation
26. Uspring
27. Young Entrepreneur
28. CompanyLoop
29. Doostang
30. Konnects
31. PairUp
32. Spoke