Threat Group-4127 Targets Hillary Clinton Presidential Campaign

secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign

- **Author:** SecureWorks Counter Threat Unit™ Threat Intelligence

- **Date:** 16 June 2016

Summary

SecureWorks® Counter Threat Unit™ (CTU) researchers track the activities of Threat Group-4127[1] (TG-4127), which targets governments, military, and international non-governmental organizations (NGOs). Components of TG-4127 operations have been reported under the names APT28, Sofacy, Sednit, and Pawn Storm. CTU™ researchers assess with moderate confidence that the group is operating from the Russian Federation and is gathering intelligence on behalf of the Russian government.

Between October 2015 and May 2016, CTU researchers analyzed 8,909 Bitly links that targeted 3,907 individual Gmail accounts and corporate and organizational email accounts that use Gmail as a service. In March 2016, CTU researchers identified a spearphishing campaign using Bitly accounts to shorten malicious URLs. The targets were similar to a 2015 TG-4127 campaign — individuals in Russia and the former Soviet states, current and former military and government personnel in the U.S. and Europe, individuals working in the defense and government supply chain, and authors and journalists — but also included email accounts linked to the November 2016 United States presidential election. Specific targets include staff working for or associated with Hillary Clinton's presidential campaign and the Democratic National Committee (DNC), including individuals managing Clinton's communications, travel, campaign finances, and advising her on policy.

Spearphishing details

The short links in the spearphishing emails redirected victims to a TG-4127-controlled URL that spoofed a legitimate Google domain. A Base64-encoded string containing the victim's full email address is passed with this URL, prepopulating a fake Google login page displayed to the victim. If a victim enters their credentials, TG-4127 can establish a session with Google and access the victim's account. The threat actors may be able to keep this session alive and maintain persistent access.

Hillary for America

The Hillary for America presidential campaign owns the hillaryclinton.com domain, which is used for the campaign website (www.hillaryclinton.com) and for email addresses used by campaign staff. An examination of the hillaryclinton.com DNS records shows that the domain's MX records, which indicate the mail server used by the domain, point to aspmx.l.google.com, the mail server used by Google Apps. Google Apps allows organizations to use Gmail as their organizational mail solution.

TG-4127 exploited the Hillary for America campaign's use of Gmail and leveraged campaign employees' expectation of the standard Gmail login page to access their email account. When presented with TG-4127's spoofed login page (see Figure 1), victims might be convinced it was the legitimate login page for their hillaryclinton.com email account.

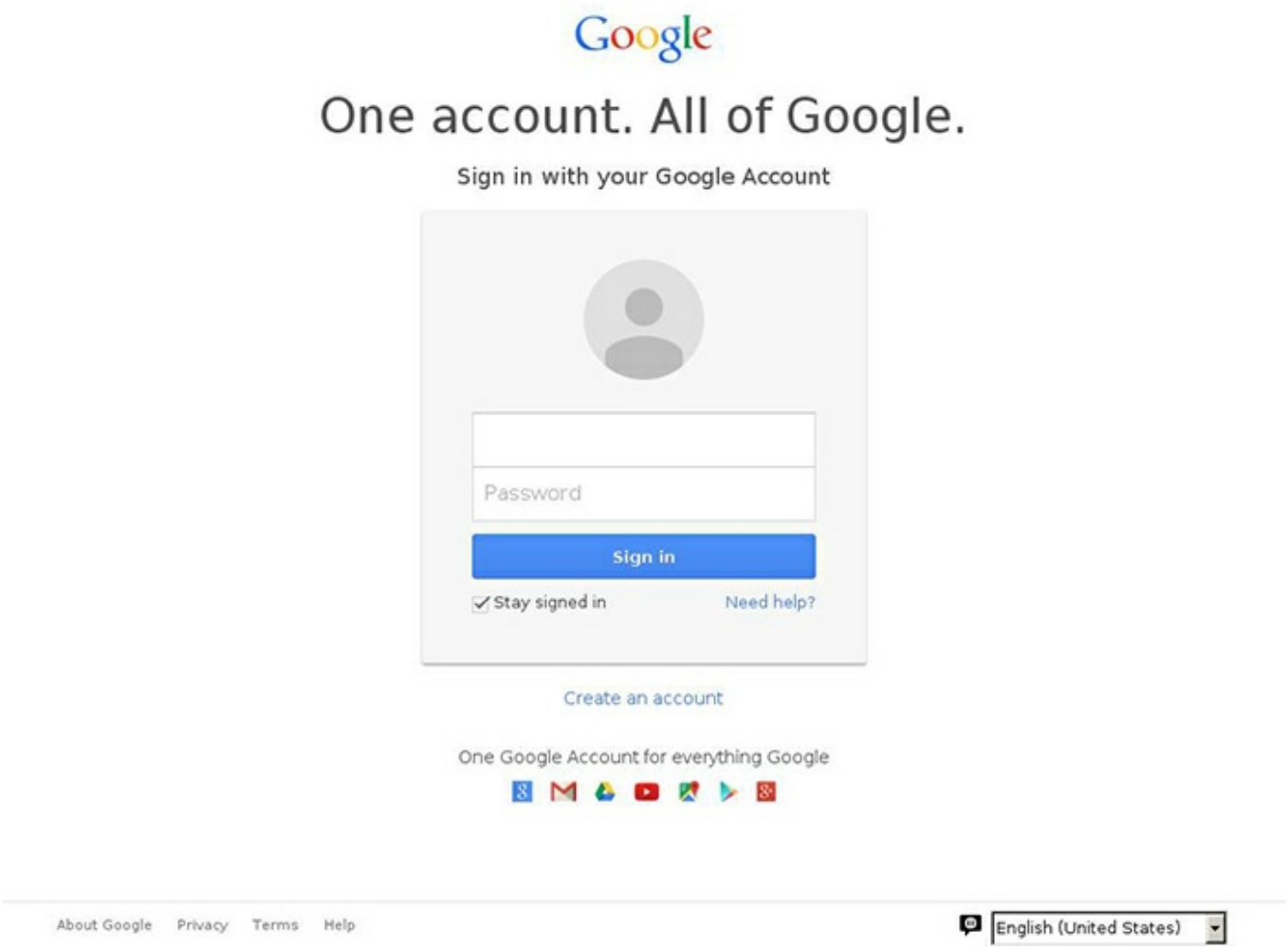

Figure 1. Example of a TG-4127 fake Google Account login page. (Source: www.phishtank.com)

CTU researchers observed the first short links targeting hillaryclinton.com email addresses being created in mid-March 2016; the last link was created in mid-May. During this period, TG-4127 created 213 short links targeting 108 email addresses on the hillaryclinton.com domain. Through open-source research, CTU researchers identified the owners of 66 of the targeted email addresses. There was no open-source footprint for the remaining 42 addresses, suggesting that TG-4127 acquired them from another source, possibly other intelligence activity.

The identified email owners held a wide range of responsibilities within the Hillary for America campaign, extending from senior figures to junior employees and the group mailboxes for various regional offices. Targeted senior figures managed communications and media affairs, policy, speech writing, finance, and travel, while junior figures arranged schedules and travel for Hillary Clinton's campaign trail. Targets held the following titles:

- National political director
- Finance director
- Director of strategic communications
- Director of scheduling
- Director of travel
- Traveling press secretary
- Travel coordinator

Publicly available Bitly data reveals how many of the short links were clicked, likely by a victim opening a

spearphishing email and clicking the link to the fake Gmail login page. Only 20 of the 213 short links have been clicked as of this publication. Eleven of the links were clicked once, four were clicked twice, two were clicked three times, and two were clicked four times.

Democratic National Committee

The U.S. Democratic party's governing body, the Democratic National Committee (DNC), uses the dnc.org domain for its staff email. Between mid-March and mid-April 2016, TG-4127 created 16 short links targeting nine dnc.org email accounts. CTU researchers identified the owners of three of these accounts; two belonged to the DNC's secretary emeritus, and one belonged to the communications director. Four of the 16 short links were clicked, three by the senior staff members. As of this publication, dnc.org does not use the Google Apps Gmail email service. However, because dnc.org email accounts were targeted in the same way as hillaryclinton.com accounts, it is likely that dnc.org did use Gmail at that time and later moved to a different service.

CTU researchers do not have evidence that these spearphishing emails are connected to the DNC network compromise that was revealed on June 14. However, a coincidence seems unlikely, and CTU researchers suspect that TG-4127 used the spearphishing emails or similar techniques to gain an initial foothold in the DNC network.

Personal email accounts

CTU researchers identified TG-4127 targeting 26 personal gmail.com accounts belonging to individuals linked to the Hillary for America campaign, the DNC, or other aspects of U.S. national politics. Five of the individuals also had a hillaryclinton.com email account that was targeted by TG-4127. Many of these individuals held communications, media, finance, or policy roles. They include the director of speechwriting for Hillary for America and the deputy director office of the chair at the DNC. TG-4127 created 150 short links targeting this group. As of this publication, 40 of the links have been clicked at least once.

Related activity and implications

Although the 2015 campaign did not focus on individuals associated with U.S. politics, open-source evidence suggests that TG-4127 targeted individuals connected to the U.S. White House in early 2015. The threat group also reportedly targeted the German parliament and German Chancellor Angela Merkel's Christian Democratic Union party. CTU researchers have not observed TG-4127 use this technique (using Bitly short links) to target the U.S. Republican party or the other U.S. presidential candidates whose campaigns were active between mid-March and mid-May: Donald Trump, Bernie Sanders, Ted Cruz, Marco Rubio, and John Kasich. However, the following email domains do not use Google mail servers and may have been targeted by other means:

- gop.com — used by the Republican National Committee
- donaldjtrump.com — used by the Donald Trump campaign
- johnkasich.com — used by the John Kasich campaign

Access to targets' Google accounts allows TG-4127 to review internal emails and potentially access other Google Apps services used by these organizations, such as Google Drive. In addition to the value of the intelligence, the threat actors could also exploit this access for other malicious activity, such as generating spearphishing emails from internal email addresses to compromise the organizations' networks with malware.

The Russian government views the U.S. as a strategic rival and is known to task its intelligence agencies with gathering confidential information about individuals and organizations close to the center of power in the U.S. Individuals working for the Hillary for America campaign could have information about proposed policies for a Clinton presidency, including foreign-policy positions, which would be valuable to the Russian government. Information about travel plans and campaign scheduling could provide short-term opportunities for other intelligence operations.

Long-term access to email accounts of senior campaign advisors, who may be appointed to staff positions in a Clinton administration, could provide TG-4127 and the Russian government with access to those individual's accounts.

Conclusion

While TG-4127 continues to primarily threaten organizations and individuals operating in Russia and former Soviet states, this campaign illustrates its willingness to expand its scope to other targets that have intelligence of interest to the Russian government. Non-governmental political organizations may provide access to desirable national policy information, especially foreign policy, but may not have the same level of protection and security as governmental organizations. Targeting individuals linked to presidential campaigns could represent an intelligence ‘long game,' as establishing access to potential U.S. administration staff before they are appointed could be easier than targeting them when they are established in the White House. Access to an individual's personal or corporate email account provides a substantial amount of useful intelligence, and threat actors could also leverage the access to launch additional attacks to penetrate the network of an associated organization.

Users rarely check the full URL associated with short links, so threat groups can use URL-shortening services to effectively hide malicious URLs. Threat actors can use the services' detailed statistics about which links were clicked when, and from what location, to track the success of a spearphishing campaign. A single compromised account could allow TG-4127 to achieve its operational goals. CTU researchers recommend that clients take appropriate precautions to minimize the risk of these types of attacks:

- Educate users about the risks of spearphishing emails.
- Use caution and exercise due diligence when faced with a shortened link, especially in unsolicited email messages. Pasting Bitly URLs, appended with a plus sign, into the address bar of a web browser reveals the full URL.
- For clients using Gmail as a corporate mail solution, educate users about the risk of spoofed login pages and encourage them to confirm they are on the legitimate Google Accounts page when presented with a Google login prompt.

Appendix — Gauging confidence level

CTU researchers have adopted the grading system published by the U.S. Office of the Director of National Intelligence to indicate confidence in their assessments:

- **High confidence** generally indicates that judgments are based on high-quality information, and/or that the nature of the issue makes it possible to render a solid judgment. A "high confidence" judgment is not a fact or a certainty, however, and such judgments still carry a risk of being wrong.
- **Moderate confidence** generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.
- **Low confidence** generally means that the information's credibility and/or plausibility is questionable, or that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that [there are] significant concerns or problems with the sources.

[1] The SecureWorks Counter Threat Unit (CTU) research team tracks threat groups by assigning them four-digit randomized numbers (4127 in this case), and compiles information from external sources and from first-hand incident response observations.