THREAT ANALYSIS

Threat Group-4127 Targets Google Accounts

SUNDAY, JUNE 26, 2016
BY: SECUREWORKS COUNTER THREAT UNIT THREAT INTELLIGENCE

- Author: SecureWorks Counter Threat Unit™ Threat Intelligence

Summary

SecureWorks® Counter Threat Unit™ (CTU) researchers track the activities of Threat Group-4127[1] (TG-4127), which traditionally targets governments, military,international non-governmental organizations (NGOs), and most recently, Hillary Clinton's email. Components of TG-4127 operations have been reported under the names APT28, Sofacy, Sednit, Fancy Bear, 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.

In June 2016, CTU researchers published analysis of a TG-4127 campaign that targeted email accounts linked to Hillary Clinton's 2016 presidential campaign and the U.S. Democrat National Committee. The activity used the same technique as a 2015 spearphishing campaign that targeted more than 1,800 Google Accounts. The threat group used the Bitly URL-shortening service to hide the location of a spoofed Google login page. Many of the accounts in the 2015 campaign belonged to individuals in Russia and the former Soviet states, but some belonged to 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, particularly those with an interest in Russia. The range of targets demonstrates that the threat group poses a broad threat to individuals and groups associated with U.S. politics, to organizations and individuals in the government and defense verticals, and to those whose business involves commenting on Russia.

Spearphishing Google Accounts

In mid-2015, CTU researchers discovered TG-4127 using the accoounts-google . com

domain in spearphishing attacks targeting Google Account users. The domain was used in a phishing URL submitted to Phishtank, a website that allows users to report phishing links (see Figure 1).

Figure 1. Example of accoounts-google . com used in a phishing URL. (Source: www.phishtank.com)

Recipients who clicked the link were presented with a fake Google Account login page (see Figure 2). The threat actors could use entered credentials to access the contents of the associated Gmail account.

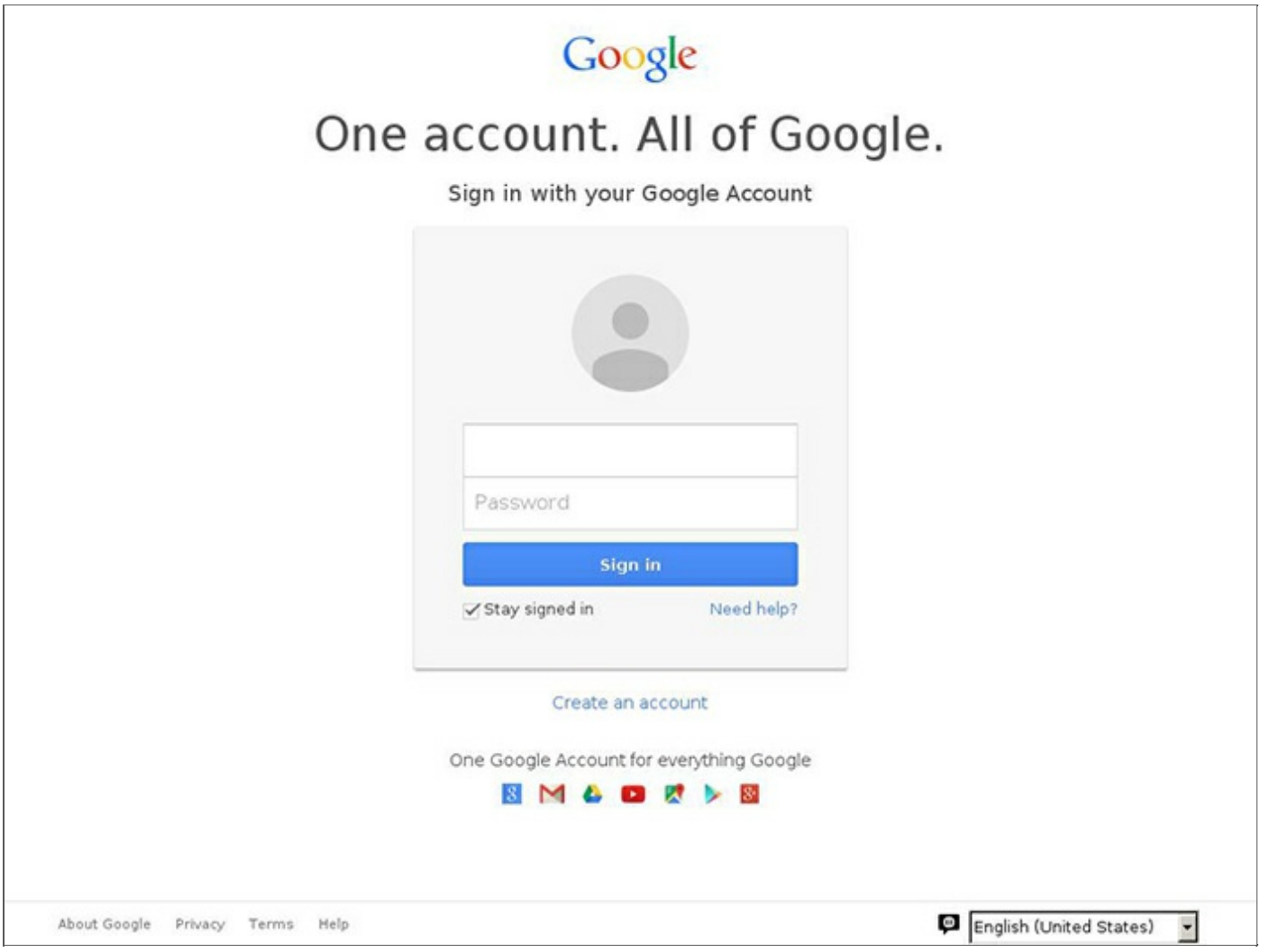


Figure 2. Fake Google Account login page. (Source: www.phishtank.com)

Encoded target details

Analysis of the phishing URL revealed that it includes two Base64-encoded values (see Figure 3). The decoded Base64 values (see Table 1) match the Gmail account and its associated Google Account username. If a target clicks the phishing link, the username field of the displayed fake Google Account login page is prepopulated with the individual's

email address.

```
http://url.googlesetting.com/url/?continue=ZGlmZWl0YWxpYS5jYW5iZXJyYUBnbWFpbC5jb20=&df=RGlmZWl0YWxpYStDYW5iZXJyYQ==&tel=1
```

Figure 3. Spearphishing URL. (Source: SecureWorks)

Base64 value	Decoded value
ZGlmZWl0YWxpYS5jYW5iZXJyYUBnbWFpbC5jb20	difeitalia.canberra @ gmail . com
RGlmZWl0YWxpYStDYW5iZXJyYQ	Difeitalia+Canberra

Table 1. Decoded Base64 values from the phishing URL used by TG-4127.

Use of the Bitly URL-shortening service

A Bitly URL was uploaded to Phishtank at almost the same time as the original spearphishing URL (see Figure 4).

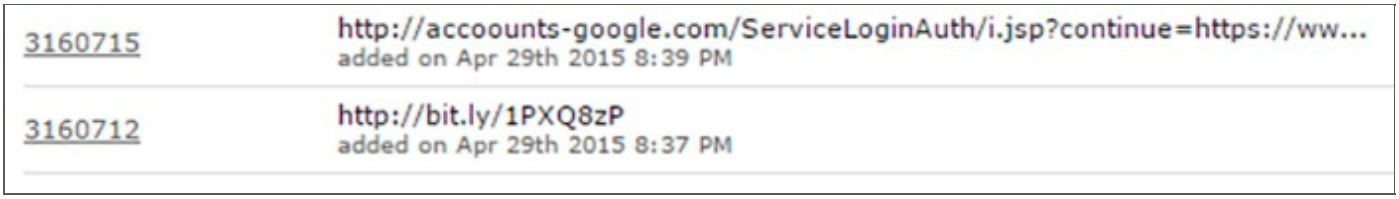


Figure 4. Bitly phishing URL submitted at same time as accoounts-google . com phishing URL. (Source: www.phishtank.com)

Using a tool on Bitly's website, CTU researchers determined that the Bitly URL redirected to the original phishing URL (see Figure 5). Analysis of activity associated with the Bitly account used to create the shortened URL revealed that it had been used to create more than 3,000 shortened links used to target more than 1,800 Google Accounts.

Figure 5. Link-shortener page for bit.ly/1PXQ8zP that reveals the full URL. (Source: www.bit.ly)

Target analysis

CTU researchers analyzed the Google Accounts targeted by TG-4127 to gain insight about the targets and the threat group's intent.

Focus on Russia and former Soviet states

Most of the targeted accounts are linked to intelligence gathering or information control within Russia or former Soviet states. The majority of the activity appears to focus on Russia's military involvement in eastern Ukraine; for example, the email address targeted by the most phishing attempts (nine) was linked to a spokesperson for the Ukrainian prime minister. Other targets included individuals in political, military, and diplomatic positions in former Soviet states, as well as journalists, human rights organizations, and regional advocacy groups in Russia.

Other targets worldwide

Analysis of targeted individuals outside of Russia and the former Soviet states revealed that they work in a wide range of industry verticals (see Figure 6). The groups can be divided into two broad categories:

- Authors, journalists, NGOs, and political activists (36%)
- Government personnel, military personnel, government supply chain, and aerospace researchers (64%)

TG-4127 likely targeted the groups in the first category because they criticized Russia. The groups in the second category may have information useful to the Russian government.

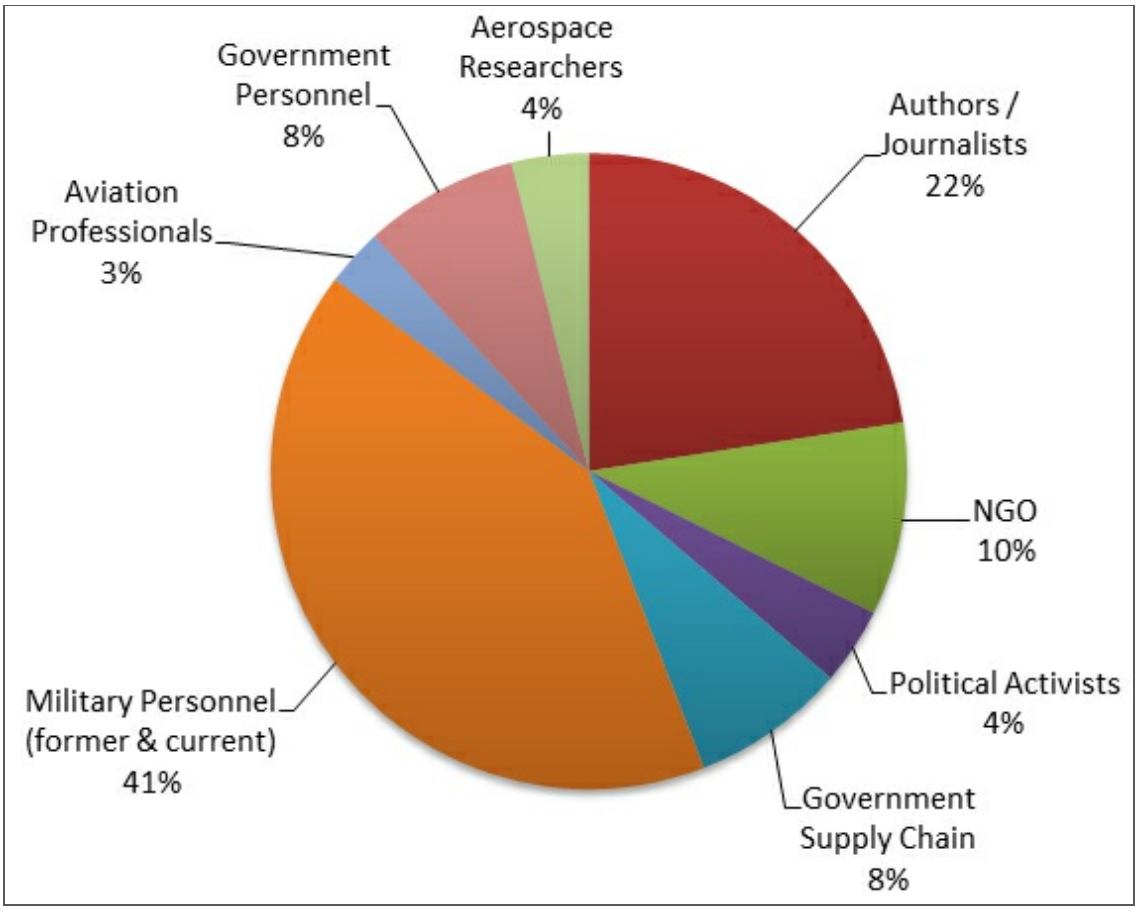


Figure 6. TG-4127 targeting outside of Russia and former Soviet states. (Source: SecureWorks)

Authors and journalists

More than half (53%) of the targeted authors and journalists are Russia or Ukraine subject matter experts (see Figure 7). It is likely that the Russian state has an interest in how it is portrayed in the media. U.S.-based military spouses who wrote online content about the military and military families were also targeted. The threat actors may have been attempting to learn about broader military issues in the U.S., or gain operational insight into the military activity of the target's spouse.

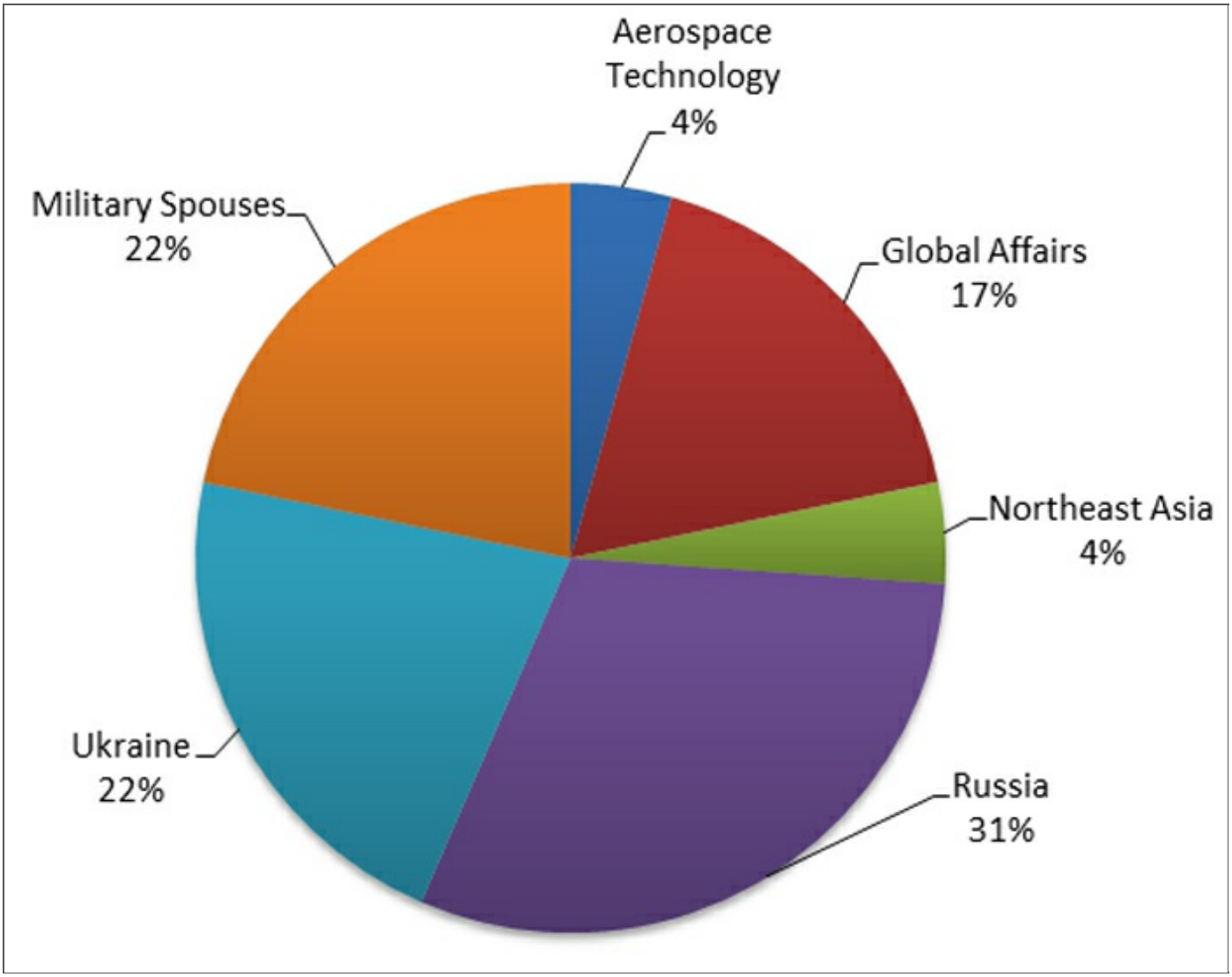


Figure 7. Subject matter expertise of authors and journalists targeted by TG-4127. (Source: SecureWorks)

Government supply chain

CTU researchers identified individuals who were likely targeted due to their position within the supply chain of organizations of interest to TG-4127 (e.g., defense and government networks). Figure 8 shows the distribution by category. The targets included a systems engineer working on a military simulation tool, a consultant specializing in unmanned aerial systems, an IT security consultant working for NATO, and a director of federal sales for the security arm of a multinational technology company. The threat actors likely aimed to exploit the individuals' access to and knowledge of government clients' information.

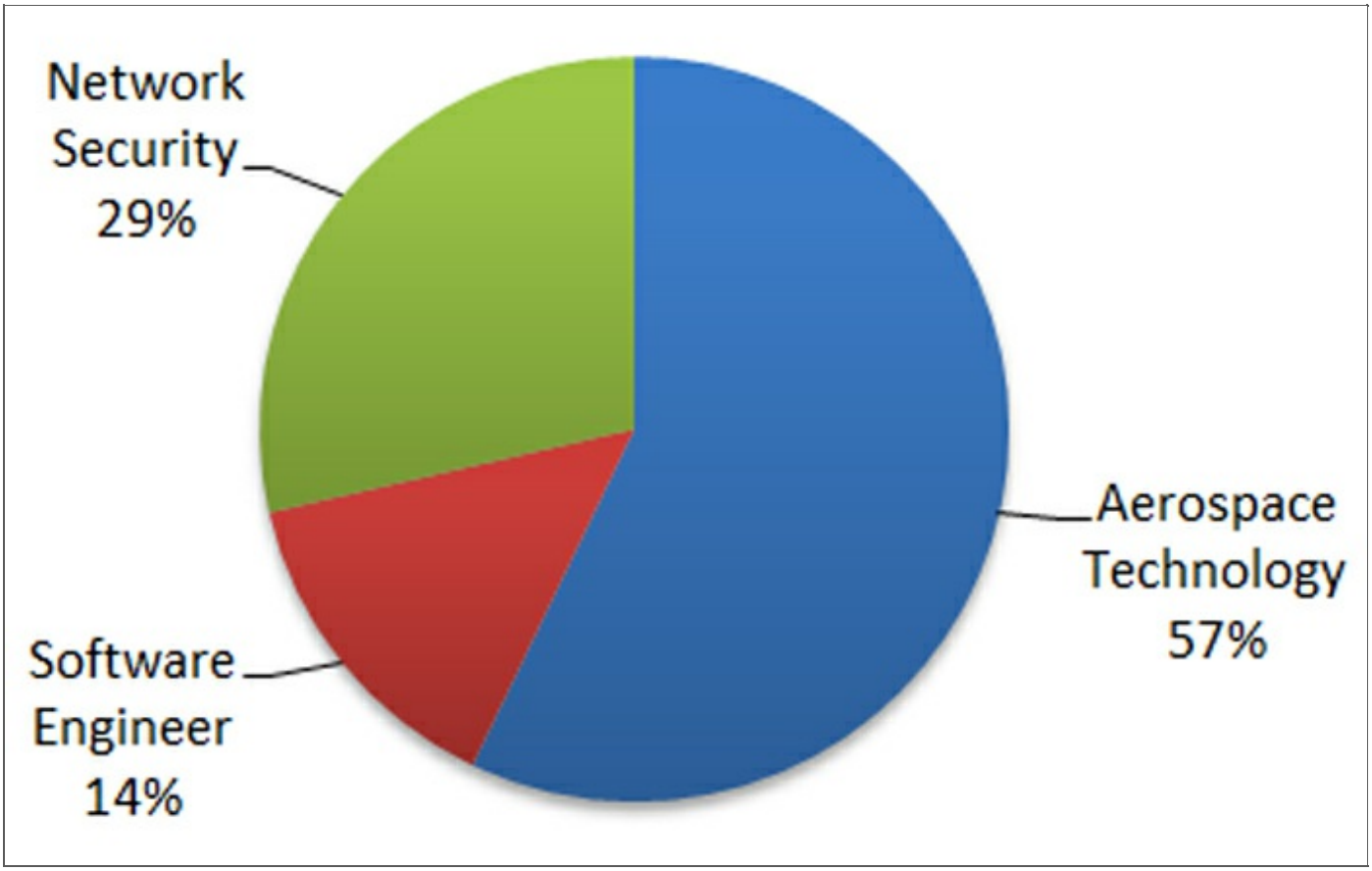


Figure 8. Categories of supply chain targets. (Source: SecureWorks)

Government / military personnel

TG-4127 likely targeted current and former military and government personnel for potential operational insight gained from access to their personal communications. Most of the activity focused on individuals based in the U.S. or working in NATO-linked roles (see Figure 9).

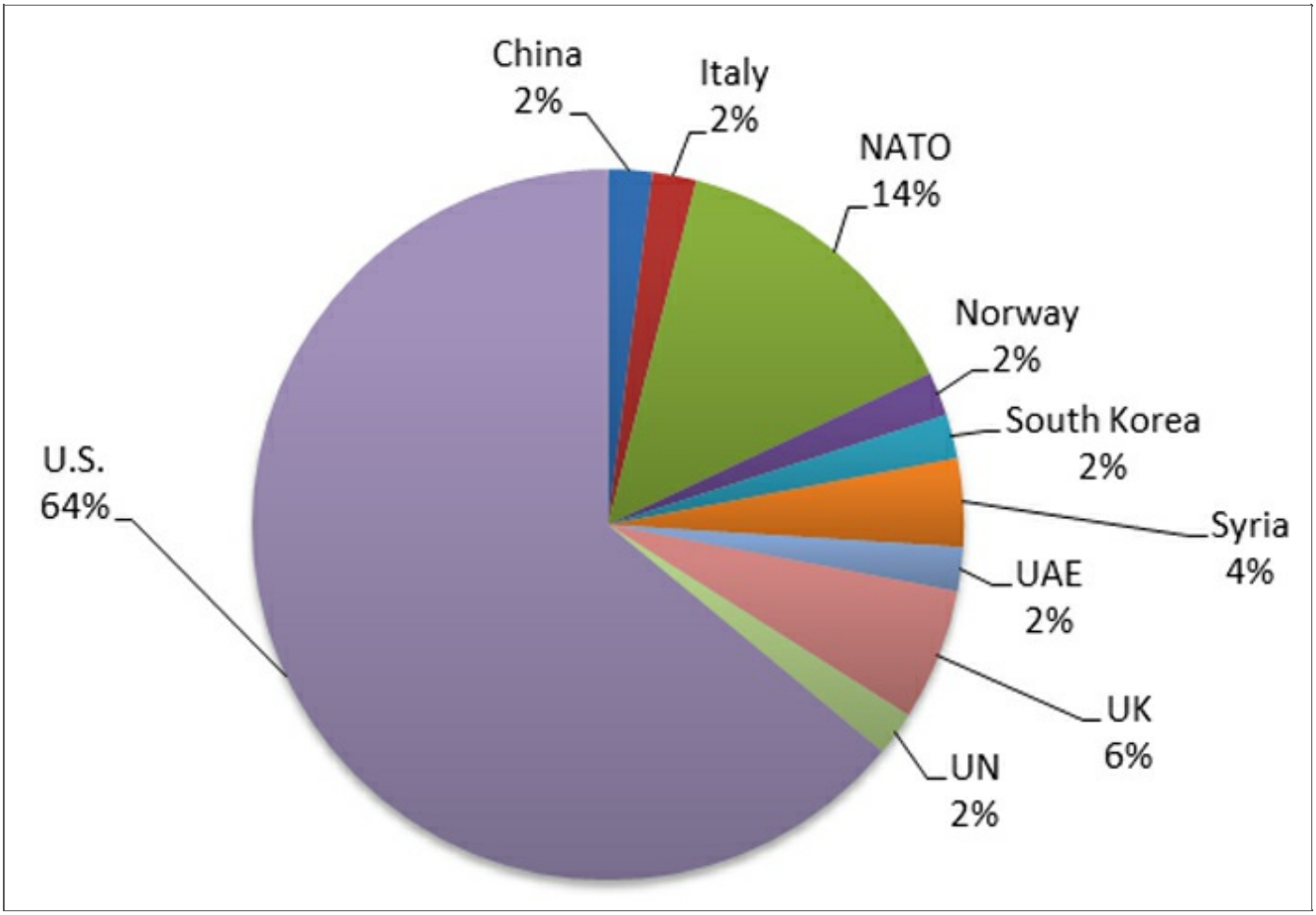


Figure 9. Nation or organization of government/military targets. (Source: SecureWorks)

TG-4127 targeted high-profile Syrian rebel leaders, including a leader of the Syrian National Coalition. Russian forces have supported Syrian President Bashar al-Assad's regime since September 2015, so it is likely the threat actors are seeking to gain intelligence on rebel forces to assist Russian and Assad regime military operations.

Success of the phishing campaign

CTU researchers analyzed 4,396 phishing URLs sent to 1,881 Google Accounts between March and September, 2015. More than half (59%) of the URLs were accessed, suggesting that the recipients at least opened the phishing page. From the available data, it is not possible to determine how many of those Google Accounts were compromised. Most of the targeted accounts received multiple phishing attempts, which may indicate that previous attempts had been unsuccessful. However, 35% of accounts that accessed the malicious link were not subject to additional attempts, possibly indicating that the compromise was successful.

Of the accounts targeted once, CTU researchers determined that 60% of the recipients clicked the malicious Bitly. Of the accounts that were targeted more than once, 57% of the recipients clicked the malicious link in the repeated attempts. These results likely encourage threat actors to make additional attempts if the initial phishing email is unsuccessful.

Conclusion

TG-4127 primarily poses a threat to organizations and individuals operating in Russia and

former Soviet states. However, a significant component of its activity targets entities in Western Europe and the U.S. The following types of individuals and organizations are at greatest risk:

- Russia subject matter experts
- Individuals and organizations that publish articles portraying Russia in a negative context
- Defense or government organizations
- Organizations and individuals involved in the government supply chain
- Former military or government personnel
- Individuals associated with U.S. politics

Users rarely check the full URL associated with URLs generated by a URL-shortening service, so threat groups can use these services to effectively hide phishing website URLs. URL-shortening services provide detailed statistics about which links were clicked when, and from what location. This information allows threat actors to track the success of a spearphishing campaign. Access to an individual's email account provides a substantial amount of useful intelligence. Threat actors could also use control of an account to launch additional attacks to penetrate the network of an associated organization.

Organizations should educate users about the risks of spearphishing and shortened links. CTU researchers recommend using caution and exercising 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.

Appendix — Gauging confidence level

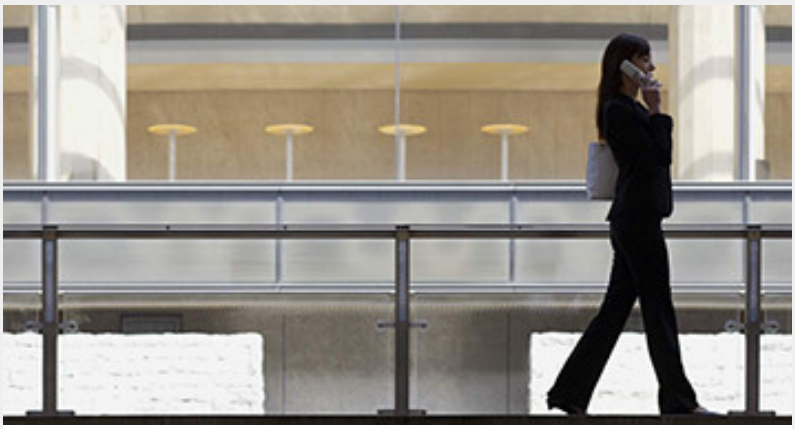
CTU researchers have adopted the grading system published by the U.S. Office of the Director of National Intelligence to indicate confidence in their assessments:

- 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.

Footnote

[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 first-hand incident response observations and from external sources.

RELATED CONTENT



BRONZE BUTLER Targets Japanese Enterprises

Counter Threat Unit™ Research Team

CTU RESEARCH