Counter Threat Unit Research Team

SUMMARY

In early 2017, SecureWorks® Counter Threat Unit™ (CTU) researchers observed phishing campaigns targeting several entities in the Middle East and North Africa (MENA), with a focus on Saudi Arabian organizations. The campaigns delivered PupyRAT, an open-source cross-platform remote access trojan (RAT). CTU™ researchers observed likely unsuccessful phishing campaigns being followed by highly targeted spearphishing and social engineering attacks from a threat actor using the name Mia Ash. Further analysis revealed a well-established collection of fake social media profiles that appear intended to build trust and rapport with potential victims. The connections associated with these profiles indicate the threat actor began using the persona to target organizations in April 2016.

CTU researchers assess that COBALT GYPSY (formerly known as TG-2889), a threat group associated with Iranian government-directed cyber operations, is likely responsible for these campaigns and the Mia Ash persona. COBALT GYPSY has used spearphishing to target telecommunications, government, defense, oil, and financial services organizations based in or affiliated with the MENA region, identifying individual victims through social media sites.

KEY POINTS

- CTU researchers assess it highly likely that the Mia Ash persona is a fake identity used to perform reconnaissance on and establish relationships with employees of targeted organizations.

- Based on perceived targeting, observed victims, and tactics used in this campaign, CTU researchers consider it likely that the COBALT GYPSY threat group manages the Mia Ash persona.

- COBALT GYPSY uses well-established social media personas and correspondence via multiple platforms to establish rapport with victims.

- Validating a user's authenticity prior to accepting social media connection requests can mitigate threats posed by threat actors leveraging fake personas.

OBSERVED ACTIVITY

Between December 28, 2016 and January 1, 2017, CTU researchers observed a phishing campaign targeting Middle Eastern organizations. The emails used various themes, but they all contained shortened URLs leading to a macro-enabled Word document. The macro ran a PowerShell command that attempted to download additional PowerShell loader scripts for PupyRAT, a research and penetration-testing tool that has been used in attacks. If installed, PupyRAT gives the threat actor full access to the victim's system.

On January 13, 2017, the purported London-based photographer "Mia Ash" used LinkedIn to contact an employee at one of the targeted organizations, stating that the inquiry was part of an exercise to reach out to people around the world. Over the next several days, the individuals exchanged messages about their professions, photography,

and travels. Sometime before January 21, Mia encouraged the employee to add her as a friend on Facebook and continue their conversation there, noting that it was her preferred communication method. The correspondence continued via email, WhatsApp, and likely Facebook until February 12, when Mia sent a Microsoft Excel document, "Copy of Photography Survey.xlsm," to the employee's personal email account. Mia encouraged the victim to open the email at work using their corporate email account so the survey would function properly. The survey contained macros that, once enabled, downloaded PupyRAT.

CTU researchers determined that the COBALT GYPSY threat group orchestrated this activity due to the tools, techniques, and procedures (TTPs) used in both campaigns. The group has repeatedly used social media, particularly LinkedIn, to identify and interact with employees at targeted organizations, and then used weaponized Excel documents to deliver RATs such as PupyRAT. The threat actors likely leveraged the Mia Ash persona to gain access to the targeted organization because the initial phishing campaign was unsuccessful.

"MIA ASH" PERSONA

CTU researchers consider it highly likely that Mia Ash is a fake persona. It is associated with LinkedIn, Facebook, Blogger, and WhatsApp accounts, as well as several email addresses. A timeline of Mia Ash activity and correspondence indicates the persona was established in April 2016 or earlier (see Appendix B). CTU analysis of these accounts revealed that most of the supporting material and content in the profiles originated from other sources.

Job description

Mia Ash's LinkedIn page contains a description of

employment at Mia's Photography that is almost identical to a job description posted on the LinkedIn account of a U.S.-based photographer (see Figure 1). It is highly likely that the threat actor copied the job description from the legitimate profile.

Photographer
Mia's Photography
January 2014 – Present (3 years 3 months) | London, United Kingdom

- Lead editor for numerous books, gallery shows, and images for media and multimedia broadcasts
- Consulted as photo editor for various International shows
- Implemented processes and structure for digital archiving, trafficked imagery, and conducted photo research and photo editing for publishing, multimedia, and exhibition projects
- Secured digital image submissions and prepared digital image priming and prepress for multi-platform projects
- Managed writing image use, photographer agreement contracts, and negotiated licensing terms and fees

Manager, Photo Editing + Image Collection + Special Projects
International League of Conservation Photographers
2009 – 2010 • 1 yr

- Lead editor for numerous books, gallery shows, and images for media and multimedia broadcasts - Selected to edit a Christies Auction House gallery of "Best Nature Photographs of All Time"
- Consulted as photo editor for Conservation International
- Implemented processes and structure for digital archiving, trafficked imagery, and conducted photo research and photo editing for publishing, multimedia, and exhibition projects such as "Freshwater: The Essence of Life"
- Secured digital image submissions and prepared digital image priming and prepress for multiplatform projects
- Managed writing image use, photographer agreement contracts, and negotiated licensing terms and fees

Figure 1. Comparison of Mia Ash job description (top) to legitimate user's job description (bottom). (Source: LinkedIn)

Images

Images of "Mia Ash" were consistent across the various accounts and profiles. They were likely taken from several social media accounts belonging to a Romanian photographer (see Appendix C). For example, the profile photograph used on the Mia Ash LinkedIn page is identical to a photograph uploaded on October 22, 2016 to the bittersweetvenom24 Instagram account, which is likely owned by the legitimate photographer. On October 30, the same photograph was uploaded to the Mia Ash Facebook account (see Figure 2).

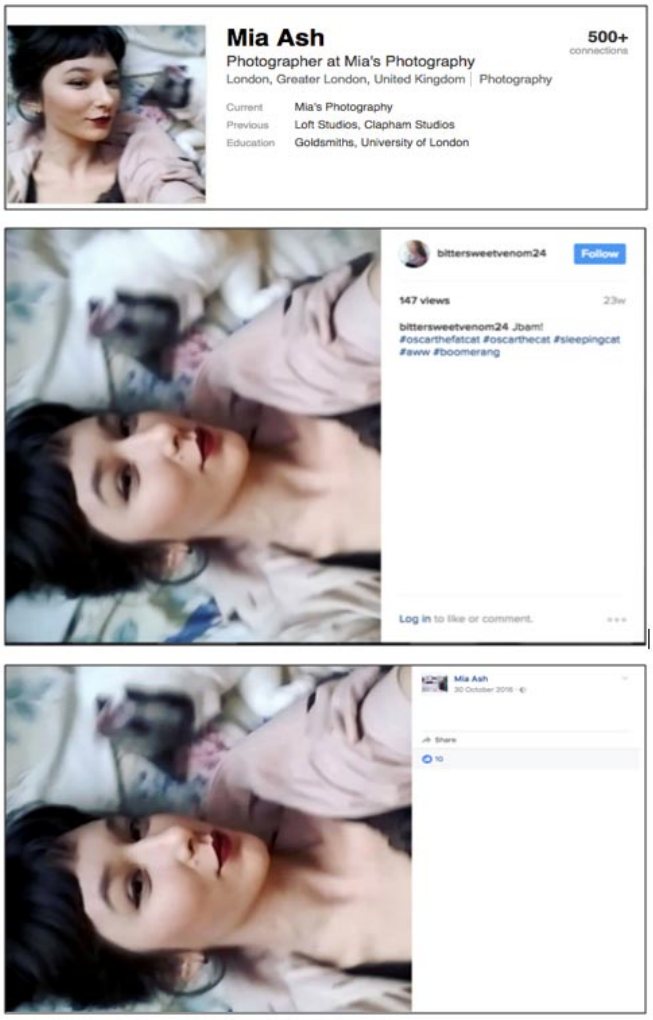

Figure 2. The same image appears on the Mia Ash LinkedIn page (top) (Source: LinkedIn), bittersweetvenom24's Instagram account (middle) (Source: https://www.instagram.com/bittersweetvenom24/), and Mia Ash's Facebook account (bottom) (Source: Facebook).

In another example, the first image uploaded to Mia Ash's Blogger site on April 2, 2016 also appears on the photographer's DeviantArt site (bittersweetvenom) (see Figure 3). The text for all of the blog posts are quotes copied from various sources. The threat actor likely created the blog to make the Mia Ash persona seem more authentic.

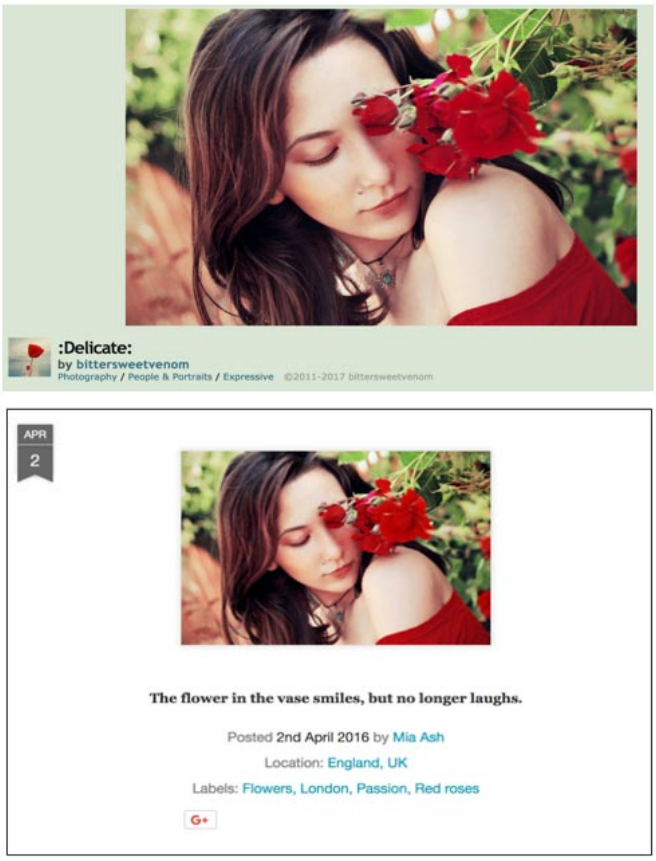

Figure 3. Image from the photographer's DeviantArt site (top) compared to an image posted to the Mia's Photography Blogger site (bottom). (Source: SecureWorks)

ATTRIBUTION

CTU researchers categorized connections associated with the Mia Ash LinkedIn profile into photography versus non-photography profiles. Several of the LinkedIn connections matched names of people associated with the Mia Ash Facebook page, which aligns with the threat actor's pattern of contacting individuals on LinkedIn and then encouraging them to move communications to Facebook. The threat actor likely used the photography connections to project authenticity. The non-photography endorsers were located in Saudi Arabia, United States, Iraq, Iran, Israel, India, and Bangladesh (see Figure 4) and worked for technology, oil/gas, healthcare, aerospace, and consulting organizations. They were mid-level employees in technical (mechanical and computer)

or project management roles with job titles such as technical support engineer, software developer, and system support. These job titles imply elevated access within the corporate network. By compromising a user account that has administrative or elevated access, threat actors can quickly access a targeted environment to achieve their objectives. The individuals' locations and industries align with previous COBALT GYPSY targeting and Iranian ideological, political, and military intelligence objectives. These characteristics suggest that COBALT GYPSY executed the January and February phishing campaigns and that it created the Mia Ash persona.

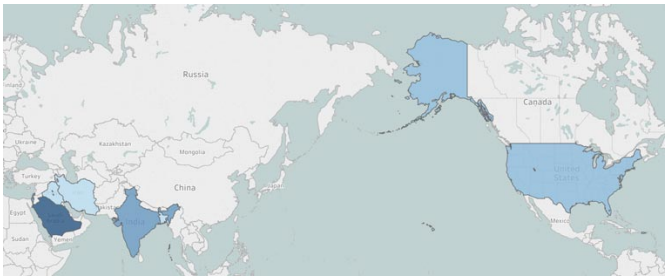

Figure 4. Mia Ash non-photography LinkedIn connections by geography. The darker the blue shading, the higher the concentration of connections from that country. (Source: SecureWorks)

CONCLUSION

CTU researchers have observed multiple COBALT GYPSY campaigns since 2015 and consider it highly likely that the group is associated with Iranian government-directed cyber operations. This threat group has launched espionage campaigns against organizations that are of strategic, political, or economic importance to Iranian interests.

The use of the Mia Ash persona demonstrates the creativity and persistence that threat actors employ to compromise targets. CTU researchers conclude that COBALT GYPSY created the persona to gain unauthorized access to targeted computer networks via social engineering. It is likely one of many personas managed by the threat actor. The

persistent use of social media to identify and manipulate victims indicates that COBALT GYPSY successfully achieves its objectives using this tactic.

COBALT GYPSY's continued social media use reinforces the importance of recurring social engineering training. Organizations must provide employees with clear social media guidance and instructions for reporting potential phishing messages received through corporate email, personal email, and social media platforms. Guidance should include recommendations for reporting inquiries by an unknown third party about an employer, business systems, or the corporate network, or requests to perform actions such as opening a document or visiting a website. CTU researchers recommend that organizations disable macros in Microsoft Office products to mitigate the threat posed by weaponized Microsoft Office documents. Organizations should also incorporate advanced malware prevention technology and endpoint threat detection tools as part of their security strategies.

APPENDIX A — IDENTIFYING ATTRIBUTION

In most cases, CTU researchers do not have intelligence to directly attribute a threat group, so attribution relies on circumstantial evidence and is an assessment rather than a fact. CTU researchers draw on three distinct intelligence bases for evidence of attribution:

- Observed activity is gathered from CTU researchers' observation and investigation of a threat group's activity on a target network and across SecureWorks data, and analysis of tactics, techniques, and procedures (TTPs) the threat group employs.

- Third-party intelligence is gained from trusted relationships within the security industry and with other private and public sector organizations, as well as analysis of open source intelligence.

- Contextual analysis compares threat group targets against intelligence requirements of government agencies and other threat actors and compares tradecraft employed by a threat group to tradecraft of known threat actors.

APPENDIX B — SAMPLE ACTIVITY FOR MIA ASH PERSONA

The timeline in Figure 5 highlights sample activity involving the Mia Ash persona, including activity associated with two victims.

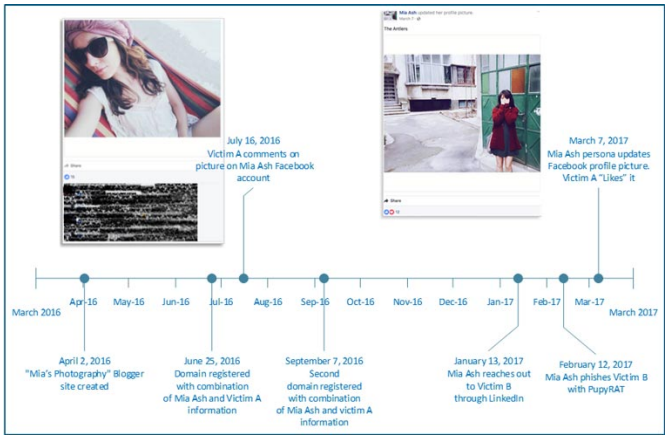

Figure 5. Timeline of Mia Ash activity. (Source: SecureWorks)

Victim A

Victim A has many social media accounts, and the profiles divulge numerous personal details. These accounts span multiple platforms; for example:

- LinkedIn
- Facebook (two accounts)
- WordPress
- Twitter
- Blogger
- Instagram

It is highly likely that Victim A is a legitimate user who operates these accounts. According to several of the profiles, Victim A has more than ten years of experience in industries such as oil/gas, aviation, and telecommunications. Victim A's location, stated areas of expertise, and listed job titles align with CTU analysis of COBALT GYPSY's interests and targets.

CTU researchers are unclear why domains were registered using a combination of Mia Ash and Victim A's information. The following are possible explanations:

- Victim A registered a domain for Mia Ash as a gesture, and the threat actor reciprocated by registering a domain for Victim A to keep Victim A as an active unknown participant in the threat actor's operations.
- The threat actor compromised Victim A's accounts.
- Victim A registered both domains as a romantic or friendly gesture.
- Domains were registered using fraudulent information.
- Victim A works for the threat actor.

CTU researchers do not know what date Mia Ash and Victim A established contact, but the timeline of associated activity indicates it was prior to the domain registrations in June 2016. The CTU research team has limited visibility into communications between the individuals, but they are likely in contact as of this publication.

Victim B

Victim B received the February 12, 2017 phishing email containing the malicious Microsoft Excel document (see the Observed activity section).

APPENDIX C — THE PHOTOGRAPHER

The images used in the Mia Ash profile likely belong to a student and photographer whose DeviantArt profile indicates is based in Romania (see Figure 6). She has uploaded hundreds of photographs of herself to social media sites such as DeviantArt, Instagram, and Facebook, leading CTU researchers

to conclude that she is who she claims to be and that the photographs on the bittersweetvenom social media profiles are of her. The threat actors operating the Mia Ash persona likely stole images from the photographer's social media accounts to create Mia Ash's various accounts. CTU researchers attempted to contact the photographer but have not received a response as of this publication.

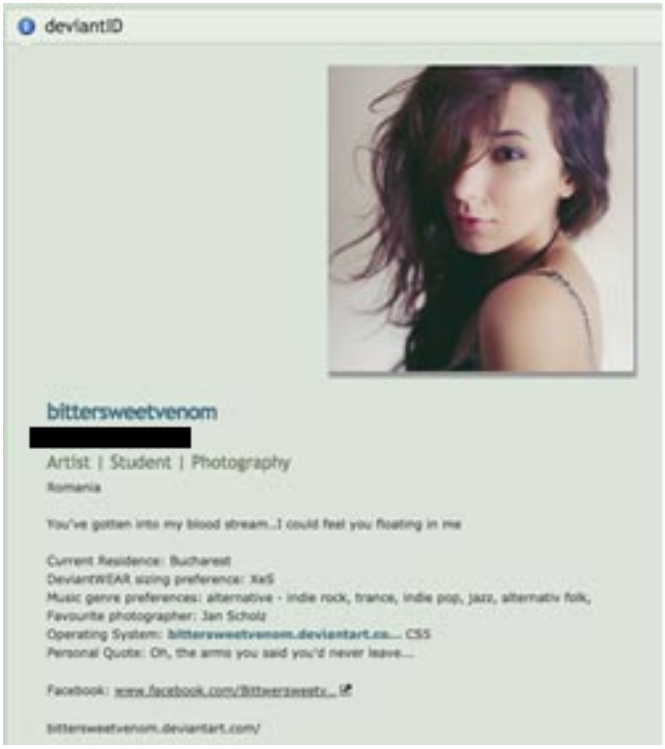

Figure 6. DeviantArt profile of "bittersweetvenom." (Source: DeviantArt.com)

TAGS: Threat Analysis Research

BACK TO MORE THREAT ANALYSES AND ADVISORIES

ADDITIONAL RESOURCES

BLOG

INFINIOS PARTNERS WITH SECUREWORKS FOR STRONGER CYBERSECURITY

READ NOW

BLOG

FIVE KEYS

READ NOW