PROJECTM: LINK FOUND BETWEEN PAKISTANI ACTOR AND OPERATION TRANSPARENT TRIBE

POSTED BY: Robert Falcone and Simon Conant on March 25, 2016 10:00 AM

FILED IN: Threat Prevention, Unit 42
TAGGED: Operation C-Major, Operation Transparent Tribe, ProjectM, Trojan

Be the first to receive the latest news, cyber threat intelligence and research from Unit 42. Subscribe Now.

Unit 42 is currently researching an attack campaign that targets government and military personnel of India. This attack appears to overlap with the Operation Transparent Tribe and Operation C-Major campaigns that targeted Indian embassies in Saudi Arabia and Kazakhstan, as well as the Indian military.

We are tracking the group of actors involved in this campaign as 'ProjectM.' During our research, we found a linkage between the infrastructure used by ProjectM and an individual from Pakistan. We cannot definitively confirm this individual is involved with this attack campaign, but the evidence that we will discuss in this blog post suggests that it is highly likely that this individual has some involvement with the threat group.

This blog post highlights the trail of evidence individuals leave on the Internet when they are not careful about disguising their identity. All of the information collected about this actor is public and accessible through open source research.

OVERVIEW OF TRANSPARENT TRIBE

The ProjectM actors rely on both spear-phishing emails and watering hole sites to deliver a variety of different tools to target the Indian government and military. ProjectM actors used a blog with a theme related to the Indian military titled "India News Tribe" (intribune.blogspot.com) as a watering hole to deliver their payloads. This group also used spear-phishing emails with malicious RTF files exploiting CVE-2010-3333 or CVE-2012-0158, in addition to Excel files that contained malicious macros to download and install their payloads as well.

The actors have access to a sizeable toolset of Trojans that they use in their attack campaigns, including custom developed tools called Crimson and Peppy, along with off-the-shelf remote administration tools (RATs) and downloaders, such as DarkComet and Bozok. Another interesting part of this campaign is the use of techniques and Trojans often seen in cybercrime attacks, such as the use of the Andromeda Trojan as an initial payload in their attacks to download and execute other tools in their toolset. The Operation Transparent Tribe report by Darien Huss of Proofpoint provides an excellent analysis of the various tools used by this group, including Crimson and Peppy and their associated infrastructure.

REGISTRATION SLIP UP

During our research, we analyzed the registration information of the Andromeda, Crimson and Peppy Trojan command and control domains used by ProjectM. A majority of the infrastructure associated with ProjectM was registered using WHOIS protection services, which conceals the actual registrant's information (name, email, etc.) used to register the domain name. However, we discovered that the actors had in all likelihood, inadvertently neglected to use WHOIS protection on two domains in their infrastructure that they used to host C2 servers for the Andromeda Trojan.

The two undisguised domains were "winupdater[.]info" and "ordering-checks[.]com", which were registered using the email address "mshoaib.yaseen [at] gmail.com", as seen in Figure 1. The Andromeda samples used these undisguised domains to deliver Peppy Trojans that used the previously observed ProjectM domain "bbmdroid.com" as a C2 server. The email address and information used to register these domains appears to be real and associated with the actor, which differs from most infrastructure used in targeted attacks that use fake information and a disposable email account during registration. On August 5, 2014, the actor seemingly discovered his mistake as the "ordering-checks[.]com" domain was updated with WHOIS protection.

Home
Government
Partners
Unit 42 Threat Intelligence
Technical Documentation
Advanced Endpoint Protection

RECENT POSTS
Ignite 2016: Conquering the Cyber Range
posted by Chad Berndtson on April 6, 2016
How the New PAN-OS 7.1 Release Benefits Government Organizations
posted by Pamela Warren on April 6, 2016
Ignite 2016: A Next-Generation Security Platform Built for the Prevention Age
posted by Chad Berndtson on April 5, 2016
Announcing PAN-OS 7.1: Extending Breach Prevention to the Cloud
posted by Chris Morosco on April 5, 2016
Rejoice! Eight New Books Inducted into the Cybersecurity Canon
posted by Rick Howard on April 5, 2016
MORE →

Domain Name: winupdater.info

Registrant ID: CR144993459

Registrant Name: Xtex Studios

Registrant Organization: Xtex Studios

Registrant Street: R-240 Sector 15A

Registrant City: Karachi

Registrant State/Province: Sindh

Registrant Postal Code: 74200

Registrant Country: PK

Registrant Phone: +92.3452183117

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email: mshoaib.yaseen@gmail.com

Domain Name: ordering-checks.com

Created On: 2014-02-11

Expiration Date: 2015-02-11

Registrant Name: Muhammad Kamran

Registrant Street1: R02323 Karachi

Registrant City: Karachi

Registrant State/Province: Sindh

Registrant Postal Code: 74200

Registrant Country: PK

Registrant Phone: +92 3452183117

Registrant Fax: +92 3452183117

Registrant Email: mshoaib.yaseen@gmail.com

Figure 1 WHOIS Information for Two Command and Control Domains without Whois Protection

WHO IS IN PROJECTM?

The Gmail address seen in Figure 1 is directly linked to Facebook, LinkedIn, Google+, and Skype accounts. All of the accounts have corroborative biographical content, giving us a possible identity of a potential actor, who appears to be a 26-year-old individual from Karachi, Pakistan. At this time, we cannot absolutely confirm this individual's involvement with ProjectM, Operation Transparent Tribe or Operation C-Major campaigns; however, strong evidence was discovered linking this individual's online presence to entities related to the threat group, which can be seen in the chart in Figure 2. Additionally, content posted to the social networking accounts suggest that the actor has an anti-Indian sentiment, which may be a motivating factor for the actor to participate in such attack campaigns.

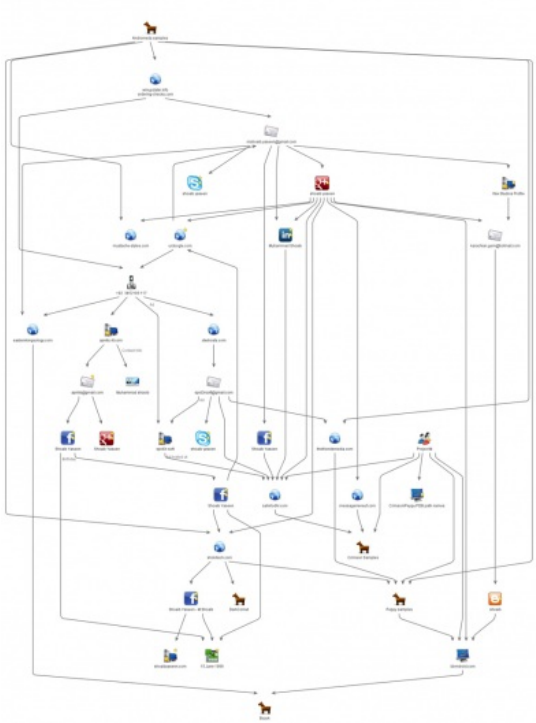

Figure 2 Diagram of links between the actor and ProjectM

WEB DESIGNER BY TRADE

We believe the individual associated with the email address “mshoaib.yaseen [at] gmail.com” was at one time and possibly still involved in web design services, as well as revenue generating efforts using Google AdSense. Interestingly, it appears that the individual reused servers and domains set up during web design efforts to host malicious content used in attack campaigns as well.

The web design and technology services company hosted at “apnits[.]4t[.]com” listed the phone number “0345-2183117” for its chief executive and as its support number. This phone number is the same as seen in the registration information in Figure 1 without the country code “+92”. We did not find any malicious content on this site; however, we did find content that suggests it was last revised in November 2006.

Another web design company created by the individual was discovered at “xtexhosts.com”. The phone number “+92.3452183117” was also found in the WHOIS information and was registered using the email “spid3rsoft [at] gmail.com”. We do not have any indication of malicious content hosted on xtexhosts.com, but it appears that the actor created it for Xtex Studios, which appears to be another web design company started by the actor.

We found a third domain, “easternkingsology[.]com,” that contained registration information with the name “Xtex Studios” and the registration email of “mshoaib.yaseen [at] gmail.com” until the domain expired in December 2015. The “easternkingsology[.]com” domain hosted a Bozok RAT sample at hxxp://easternkingsology[.]com/det/dllbb.exe (SHA256: e4dfcf3db512260e1a4ff414907610d5d5279143fa9ade9219d8691be02e512f), which suggests the threat actor hosted this Trojan on an Xtex Studios related domain for use in a ProjectM campaign. Figure 3 shows an advertisement of the services provided by Xtex Studios using “mshoaib.yaseen [at] gmail.com” and “karachian.gem [at] hotmail.com” for contact purposes.

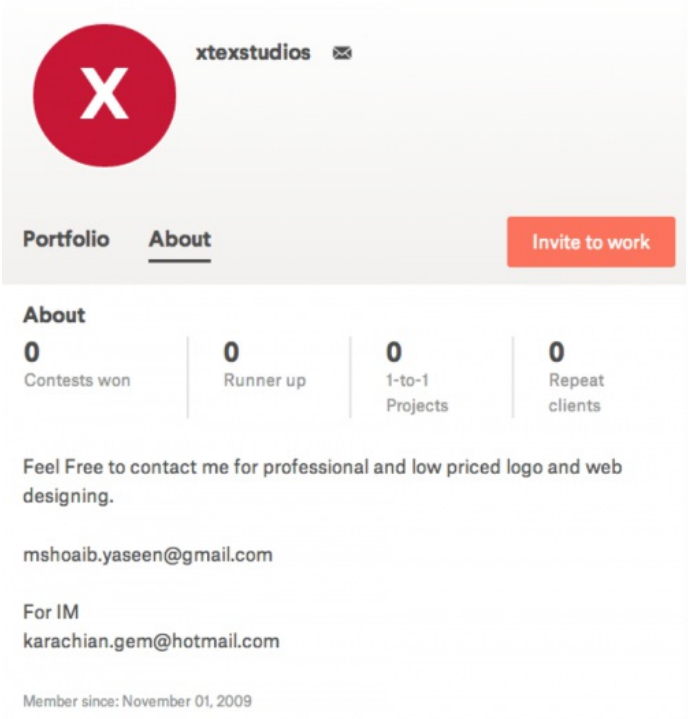

Figure 3 Website Advertising Xtex Studios Services Linking Two Email Addresses

We found the registration phone number and email address for xtexhosts[.]com on an advertisement for another web design company called SPID3R[.]SOFT. The advertisement seen in Figure 4 was hosted on “sahirlodhi[.]com”, which was a domain also used by ProjectM as the download location for a sample of the Crimson tool. At first we hypothesized that sahirlodhi[.]com may have been a compromised site, as it appeared to be the official site for the Pakistani television actor Sahir Lodhi. On May 10, 2008, the domain registration information was updated to include the registrant email of “mshoaib.yaseen[at]gmail.com”, suggesting the threat actor was involved in the creation of this website. The registration information for this domain remained the same until May 21, 2014 when it was updated to include WHOIS privacy protection. We believe that the threat actor still had access to the sahirlodhi[.]com webserver and used it to host the payload for ProjectM, further suggesting that the actor reuses domains and servers to host content and payloads unrelated to its original purpose.

Figure 4 Advertisement of SPID3R.SOFT Web Design

In addition to xtexhosts[.]com, the domain “thefriendsmedia[.]com” was also registered using the email “spid3rsoft[at]gmail.com”. This domain hosts a multimedia website that claims it is “Asia’s Biggest Entertainment Portal”. Unit 42 saw this domain hosting several ProjectM tools, including the exact same Andromeda and Peppy samples as those previously observed using bbmdroid[.]com as a C2, which were hosted at “/est/estma.exe” and “/est/controller.exe” respectively.

The “thefriendsmedia[.]com” site makes references to “thefriendsfm[.]com”, which was originally registered in October 2010 using the email “mshoaib.yaseen[at]gmail.com”. On March 24, 2014, the actor shared a link on his Facebook (figure 5) and Google+ accounts to an article hosted on “thefriendsfm[.]com” titled “MOD Assistant Director and Staff Grade NTS Results 2014”, which is currently still present on the “thefriendsmedia[.]com” domain. The post discusses applying for positions at the Pakistani Ministry of Defense (MOD), but we do not have any conclusive evidence that the actor applied to or is connected in anyway with the MOD.

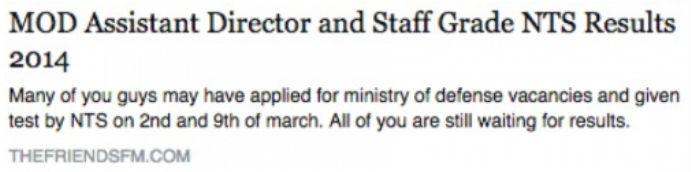

Figure 5 Actor’s Facebook post to an article regarding jobs in Pakistan’s Ministry of Defense

SOCIAL MEDIA ACTIVITY

The email address “karachian.gem[at]hotmail.com” seen in the advertisement of Xtex Studios led to the discovery of the possible identity of an individual that is likely involved with ProjectM. Unit 42 found the individual’s Google+ profile, seen in Figure 6 and noticed that the profile had several posts that included domains that had hosted payloads or were C2 servers associated with ProjectM, such as:

- bbmdroid[.]com (Peppy, Bozok)
- shobitech[.]com (Peppy, DarkComet, Andromeda)
- mustache-styles[.]com (Andromeda)
- messagerieneuf[.]com (Crimson)
- sahirlodhi[.]com (Crimson)

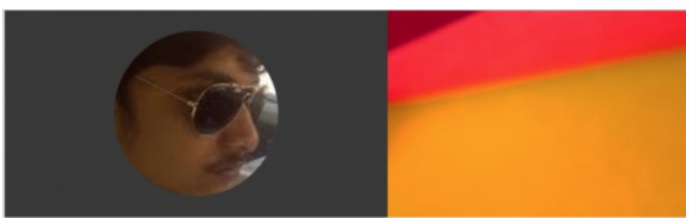

Figure 6 Possible Actor Involved with ProjectM

Also, Facebook and Google+ posts include “Bind an exe in excel file | Microsoft Excel Exploit | ShobiTech” (Figure 7), which is interesting as ProjectM has used malicious Excel delivery

documents with macros to download and install payloads in its attack campaign.

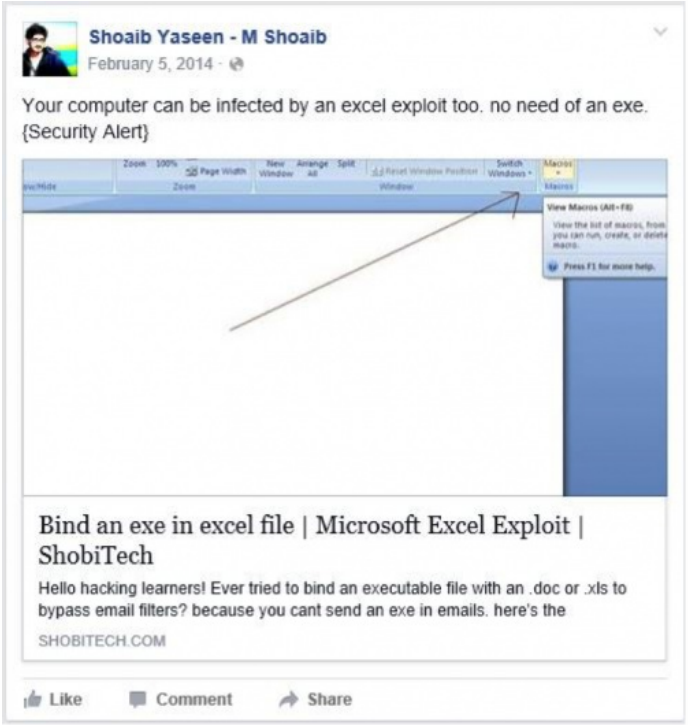

Figure 7 – Actor discusses technique seen in campaigns

The “shobitech[.]com” domain also appeared in one of the actor’s Facebook accounts. This Facebook account provided a great deal of information about the actor, specifically in the photos section. The actor used the shobitech[.]com domain in 2013 to host details of a training course (Figure 8) that he was conducting on how to monetize YouTube using Google AdSense.

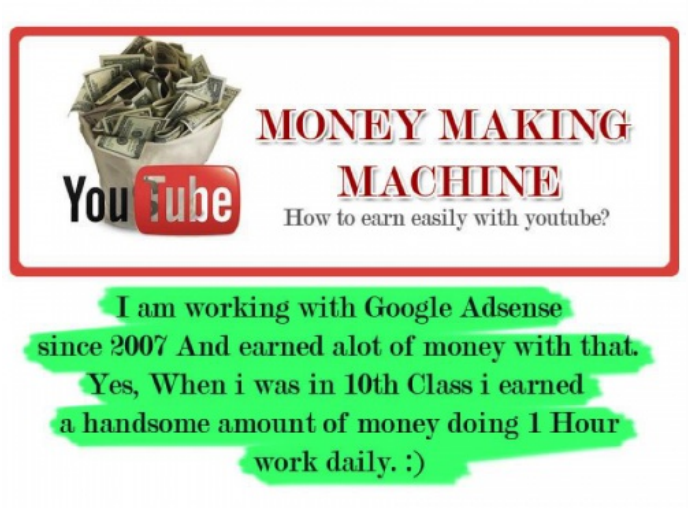

Figure 8 Advertisement Associated with a Training Conducted by Actor

The photos also show the actor obtained a certificate for completing the “Windows Exploit Development Megaprimer” online course hosted on udemy.com and screenshots of the actor using various offensive security tools, such as Metasploit on Kali Linux (Figure 9). The Operation Transparent Tribe report suggested that Meterpreter samples were used as payloads in the campaign, which is interesting as Meterpreter is part of the Metasploit Framework that the individual has had experience with according to the photos uploaded to his Facebook account.

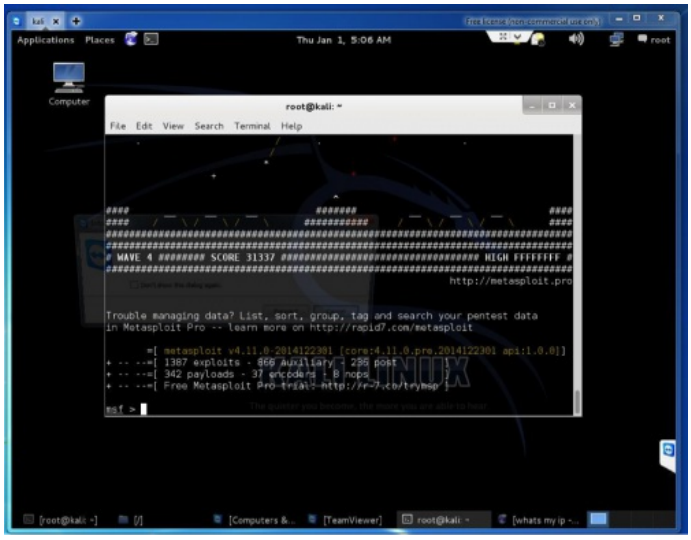

Figure 9 Photo Uploaded to Facebook Account of Individual Using Metasploit

Furthermore, another Facebook account belonging to this actor points to “shoaibyaseen[.]com”, which appears to host this individual’s personal blog. The blog has a total of twelve posts between February 29, 2016, and March 2, 2016. The topics posted to this blog include network port scanning and data gathering techniques, as well as commands to run using Metasploit and Meterpreter to accomplish various tasks to exploit systems and carry out post-exploitation activities. While the use of Meterpreter in Figure 9 and the topics in the “shoaibyaseen[.]com” blog in Figure 10 do not directly implicate this individual, it does strongly suggest that he possesses skills that would be valuable to offensive campaigns like those conducted by ProjectM.

Figure 10 Recent posts on the actor’s blog with topics including Metasploit and post exploitation activities

Another interesting observation about this actor is that his name shows up in the debug symbol path of several Crimson tools. The actor’s name appears in the debug symbol path of samples of the Crimson downloader and the remote administration tool, suggesting the actor may have been involved with the development of this Trojan. For instance, the following shows an example of the actor’s name in the debug symbol path of a Crimson downloader (SHA256: dc8bd60695070152c94cbeb5f61eca6e4309b8966f1aa9fdc2dd0ab754ad3e4c):

E:\Projects\m_project\main\mj shoaib\Thin Client\secure_scan\secure_scan\obj\x86\Debug\secure_scan.pdb

ACTOR’S EARLY BLOGGING

The email address “karachian.gem[at]hotmail.com” also led us to the individual’s blogger account, which was created in April 2008. The “About Me” section of this blogger account states that this individual lives in Karachi, Pakistan and studied computer science. This account also created several other blogs as well, most of which had little content of interest with the following exceptions:

- bbmdroid[.]blogspot[.]com
- indian-attack[.]blogspot[.]com
- Freeowlsofminerva[.]blogspot[.]com

Figure 11 Picture of Individual Associated with Blogger Accounts

The first related blog of interest is bbmdroid[.]blogspot[.]com that contains a link to "bbmdroid[.]com", which hosted C2 services for various ProjectM tools. The indian-attack[.]blogspot[.]com does not contain any malicious exploit code or payloads, but has a theme of terrorism in India. A blog with a theme related to India closely resembles the India News Tribe (intribune[.]blogspot[.]com) blog that ProjectM used in Operation Transparent Tribe to deliver Crimson payloads.

The "freeowlsofminerva[.]blogspot[.]com" blog was created on August 24, 2013, to offer a service for players of the MapleStory MMORPG. The links on the blog point to Excel spreadsheets hosted on "microsoftexcel[.]united-host[.]us", such as:

hxxp://microsoftexcel[.]united-host[.]us/Downloads/(Bera)%20FM%20Price%20List.xls

The blog also includes a link at the bottom of the page to a VirusTotal scan of a file named "(Bera) FM Price List.xlsx" that showed that no antivirus vendors detected the file as malicious. We do not have access to the spreadsheets hosted "microsoftexcel[.]united-host[.]us" to confirm if they were malicious or not; however, we did observe a DarkComet payload (SHA256: cc488690ce442e9f98bac651218f4075ca36c355d8cd83f7a9f5230970d24157) hosted on this server at "microsoftexcel[.]united-host[.]us/update.exe". The fact that a payload was hosted on this server leads us to believe the inclusion of the link to a VirusTotal analysis is a social engineering attempt to increase the likelihood a victim would click the links.

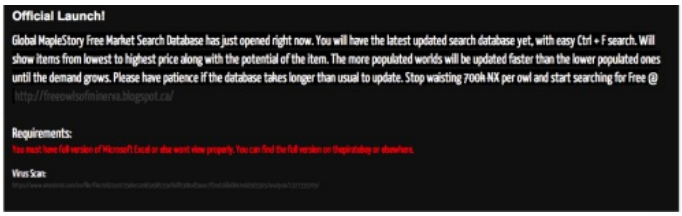

Figure 12 Use of VirusTotal Report to Increase Likelihood of Victim Clicking Links

CONCLUSION

ProjectM is a threat group conducting targeted attacks on government and military personnel of India. Unit 42 has linked several different domains within ProjectM's infrastructure to an individual residing in Pakistan. This corresponds with the suspicions of David Sancho and Feike Hacquebord at Trend Micro, who documented a likely Pakistani link to the activity in their Operation C-Major report.

At this time, we cannot elaborate on the extent of this individual's involvement with the targeted attacks; however, it does appear that the individual was involved with setting up some portion of the infrastructure used by the various payloads delivered in the attack campaign. According to the individual's social media pages and blogs, it strongly suggests he possesses skills to carry out offensive activities in ProjectM campaigns. Also, the individual's name appearing within Crimson Trojan samples suggests that he may have been involved with the creation of the malware as well.

Trend Micro reported finding gigabytes of personal identifiable information (PII) in open directories on C2 servers related to ProjectM, mostly belonging to Indian Army personnel. Although such PII might be used for financial gain, we find multiple instances in social media and blogs where this actor states anti-Indian sentiments, suggesting he is potentially politically motivated.

While knowing the identity and motivations of a possible actor is not necessarily actionable from a defensive perspective, it does provide a good reminder that people are always behind an attack, as it is easy to become fixated solely on the technical aspects of malware and infrastructure.

POST YOUR COMMENT

Name *

Email *

Website

Post Comment