Looking Into a Cyber-Attack Facilitator in the Netherlands

blog.trendmicro.com/trendlabs-security-intelligence/looking-into-a-cyber-attack-facilitator-in-the-netherlands/

Feike Hacquebord (Senior Threat Researcher)

A small web hosting provider with servers in the Netherlands and Romania has been a hotbed of targeted attacks and advanced persistent threats (APT) since early 2015. Starting from May 2015 till today we counted over 100 serious cyber attacks that originated from servers of this small provider. Pawn Storm used the servers for at least 80 high profile attacks against various governments in the US, Europe, Asia, and the Middle East. Formally the Virtual Private Server (VPS) hosting company is registered in Dubai, United Arab Emirates (UAE). But from public postings on the Internet, it is apparent that the owner doesn't really care about laws in UAE. In fact, Pawn Storm and another threat actor attacked the UAE government using servers of the VPS provider through highly targeted credential phishing. Other threat actors like DustySky (also known as the Gaza hackers) are also regularly using the VPS provider to host their command-and-control (C&C) servers and to send spear phishing e-mails.

Besides cyber-espionage and cyber attacks, this VPS provider hosts a lot of cybercrime as well. In 2014, it hosted a C&C server of the infamous Carbanak banking malware. In 2015, the hosting provider more or less invited spammers to come abuse its services when support staff posted a public post on a shady webforum saying: "sending campaigns of email marketing" is allowed. When one takes this literally there is nothing illegal or malicious there. However, "email marketing" is usually spammers' speak for e-mail spamming.

Figure 1. VPS confirming email marketing service

In 2015, the VPS provider had the notorious bulletproof hosting provider Maxided as a customer. Starting from last fall, border gateway protocol (BGP) routing tricks were applied to obscure the fact that Maxided was routing IP addresses via the VPS provider to computer servers in a datacenter in Amsterdam. In 2016 BGP routing tricks continued to obscure the view on malicious activities.

More than once, we have witnessed that the VPS provider announced small IP ranges (CIDRs) assigned to Russia or Chile for a short period of time, sometimes for a couple of days only. While these short announcements might seem like mistakes caused by fat fingers, we believe they are for malicious activities that must remain unnoticed. Indeed we have seen bursts of e-crime like phishing sites and C&C servers hosted during the time intervals the IP ranges were announced. Apparently when complaints come in or when the attack campaign has finished, the IP ranges are removed from the routing table and later the same trick starts again with another small IP range that still has a clean record.

As mentioned earlier, the postal address of the VPS company is in Dubai, but the owner makes it clear in public postings that he doesn't feel bound to laws in Dubai. In fact Pawn Storm set up very targeted credential phishing sites against the UAE government and UAE armed forces more than once on IP addresses of the VPS provider in 2015.

Elusive entity

The identity of the owner of the VPS company is unclear to us. There is a name in the public RIPE whois database and someone is using that name to post responses to queries on forums about web hosting companies. But it is unclear whether that name is real or not.

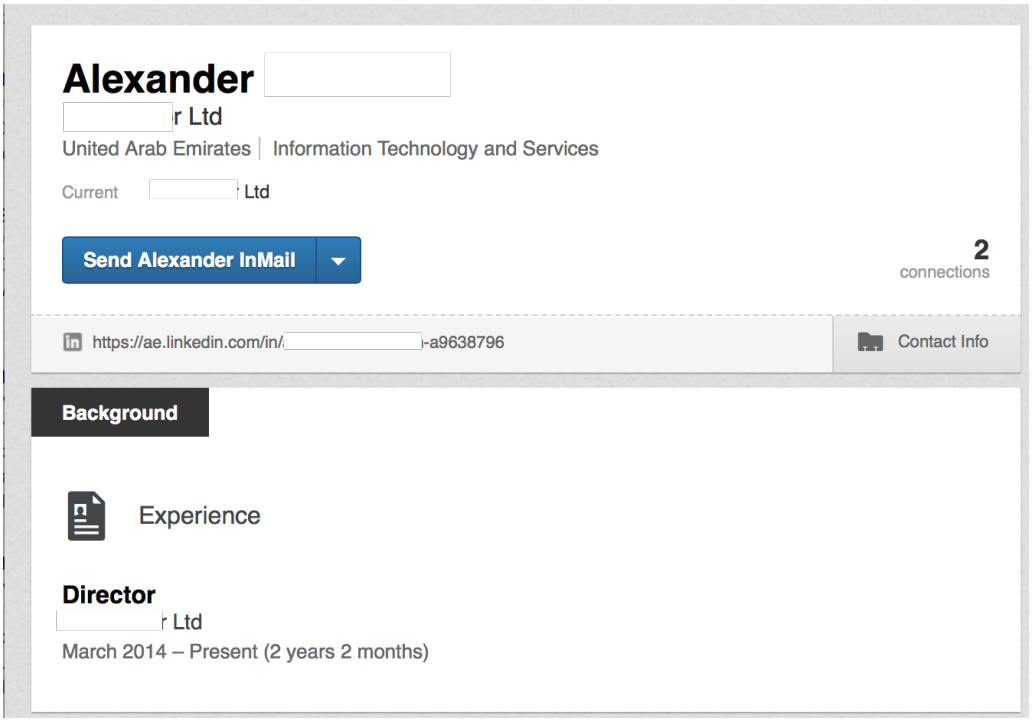


Figure 2. VPS Director Linkedin profile

The LinkedIn page of the “director” only has two connections and doesn’t show any working history. We were able to identify other persons who are working for the company. They come from the Philippines, Egypt and Palestine, indicating that the VPS provider probably uses a virtual team of employees who work remotely.

Interesting mix of customers

The mix of customers using the VPS provider for cyber attacks is interesting: Pawn Storm seems to feel quite at home. They used the VPS hosting company for at least 80 attacks since May 2015. Their attacks utilized C&C servers, exploit sites, spear-phishing campaigns, free Webmail phishing sites targeting high profile users, and very specific credential phishing sites against Government agencies of countries like Bulgaria, Greece, Malaysia, Montenegro, Poland, Qatar, Romania, Saudi Arabia, Turkey, Ukraine, and United Arab Emirates. Pawn Storm also uses the VPS provider in the Netherlands for domestic espionage in Russia regularly.

Apart from Pawn Storm, a less sophisticated group of threat actors called DustySky is using the VPS provider. These actors target Israel, companies who do business in Israel, Egypt and some other Middle Eastern governments.

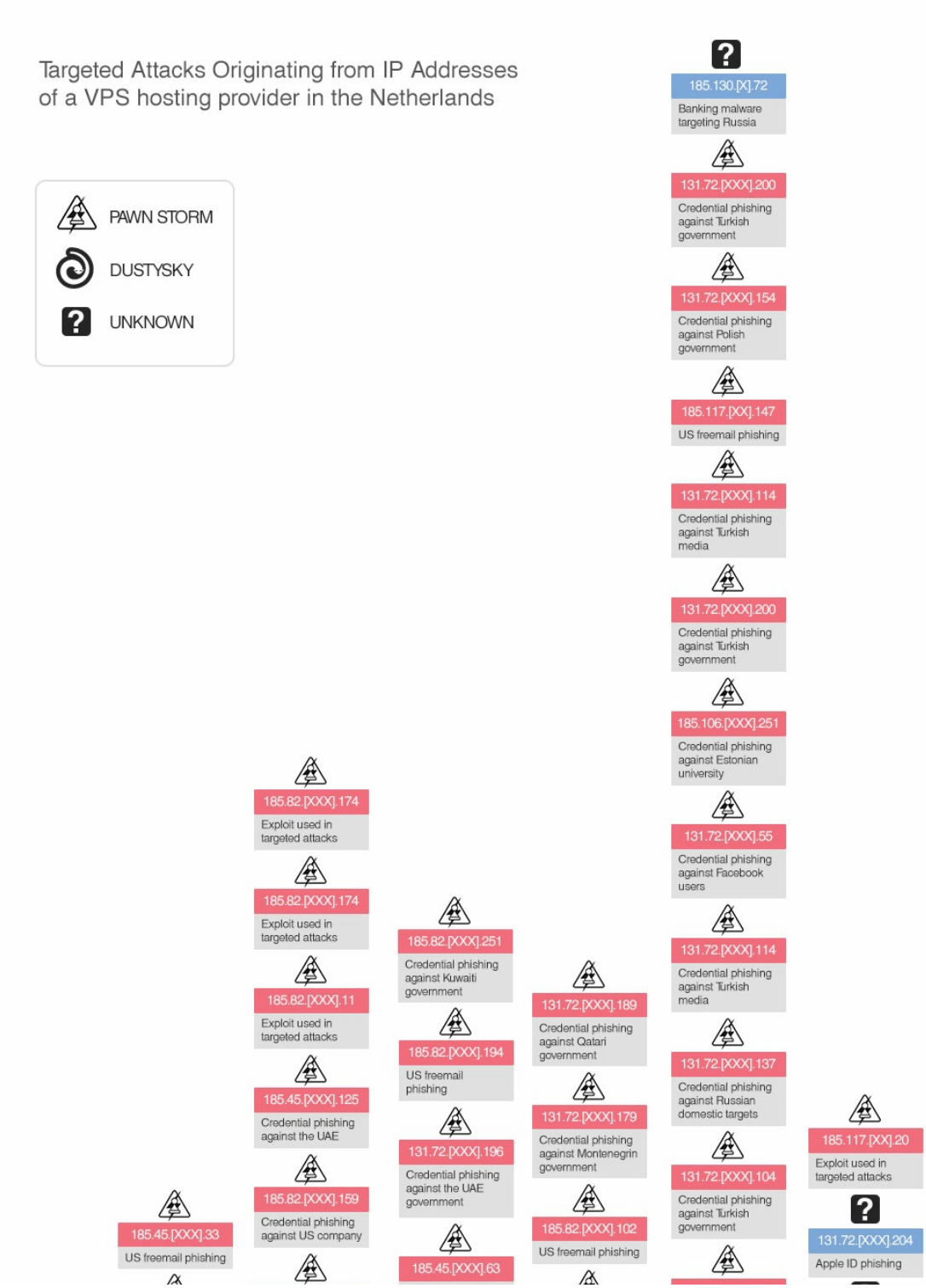
In 2016, the cybercrime *spam* problem has reduced. The VPS provider does have some legitimate customers, so the company is not 100% bulletproof in the strict sense. However, the amount of abuse continues to be high and the number of APT attacks is so staggering that this company will remain on our watchlist in the next few months.

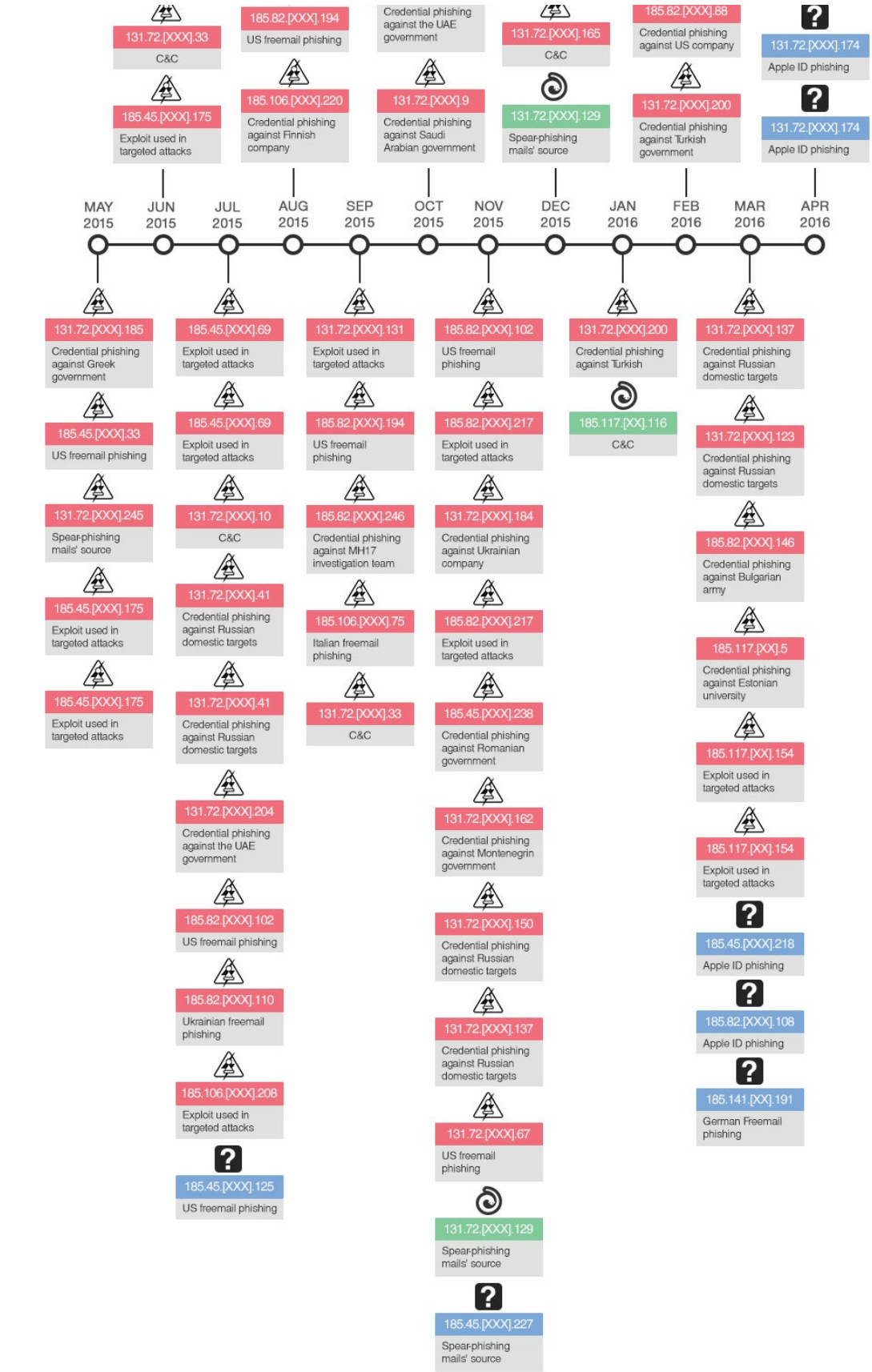
The Netherlands has good Internet connectivity and stable hosting providers. This is one of the reasons why cybercriminals and APT actors like to use servers in this country. The small VPS provider in Amsterdam is not the

only one that attracts Pawn Storm and other APT actors.

About a year ago, a hosting company from The Hague, known for its leniency in preventing outbound DDoS attacks from its network, rebranded itself to an “offshore” web hosting company with a postbox in Panama and Seychelles. Pawn Storm already found its way to the rebranded hosting company and hosted a credential phishing site targeting a state run press agency of Turkey there. The financial sector in the Netherlands has been called out by experts as vulnerable to tax evasion constructions. Is the Dutch web hosting industry vulnerable to off shore constructions that offer enhanced anonymity to cybercrime and cyber espionage?

Below is a timeline showing the attacks originating from IP addresses of a VPS hosting provider in the Netherlands. The appendix of this timeline is here.





COPYRIGHT © 2016 TREND MICRO INCORPORATED. ALL RIGHTS RESERVED.

Update as of April 21, 2016, 7:15 P.M. PDT:

The appendix was added.