[tr1adx]: Intel

tr1adx Intelligence Bulletin (TIB) 00002: The "Digital Plagiarist" Campaign: TelePorting the Carbanak Crew to a New Dimension
[January 1, 2017]

Summary

Over the past few months, the tr1adx team has been tracking a Threat Actor which we codenamed "TelePort Crew".

- We believe the "TelePort Crew" Threat Actor is operating out of Russia or Eastern Europe with the group's major motivations appearing to be financial in nature through cybercrime and/or corporate espionage.
- We have dubbed the group's latest campaign "Digital Plagiarist" for its signature practice of mirroring legitimate sites (using Tenmax's TelePort Pro and TelePort Ultra site mirroring software) onto similarly named domains, on which the TelePort Crew would host and serve up malware laden Office documents.
- The Threat Actor would then craft specific spear phishing emails to direct their targets to visit the malicious web sites and open the malware laden documents.
- Corerrelation of the TelePort Crew's TTPs and infrastructure leads us to believe the group is closely affiliated with, and may in fact be, the Carbanak Threat Actor.

At this time, we are able to disclose that we have seen activity associated with the "Digital Plagiarist" campaign in the following countries:

- Australia
- United Kingdom
- United States
- Ireland
- Switzerland
- Bahamas

Focused Industries for the "Digital Plagiarist" campaign include:

- Hospitality
- Restaurant Chains
- Food Production
- Nutritional Supplements
- Agriculture / BioTechnology
- Marketing / Public Relations
- Manufacturing
- Logistics
- Software Development (including Point-of-Sale solutions)
- Utilities & Electric
- Government

Analysis

Activity attributed to the "Digital Plagiarist" campaign first came on tr1adx's radar in the fall of 2016, when the TelePort Crew threat actor was seen registering a number of domain names which raised flags due to the suspicious nature of the domain names, attributes associated with the domain registration, and content served on these domains. Further research indicates that the "Digital Plagiarist" campaign has been active since at least July 2016, and possibly earlier, with very rapid turn around times between the provisioning of attack/C2 infrastructure and execution of the actual attacks.

Based on our observations, we believe the TelePort Crew threat actor has performed considerable research on their targets, including mapping out business/customer relationships between the targets as well as understanding other geographic and target "trust" specific attributes often seen in cases of watering hole attacks.

Overview of Attack Methodology and TTP's

Domain Registration

The TelePort Crew would start off by registering domain names, which closely resemble those of legitimate web sites. These web sites would be designed to either mimic the group's intended target, or a third party trusted by the intended target. The majority of these domain registrations appear to use a single registrar, "*PDR Ltd. d/b/a PublicDomainRegistry.com*", and in some cases the Threat Actor would recycle the same Registrant Information. We also noted a number of specific differentiators when it comes to comparing the Registrant Information and the types of malicious websites that were used.

The following table summarizes some of the more interesting domains we have seen the TelePort Crew threat actor register as part of the "Digital Plagiarist" campaign. While some of these domains are used for malware delivery, others are used for email domain spoofing, and C2 communications. A full list of (disclosable) domains suspected to be associated with the TelePort Crew's "Digital Plagiarist" campaign is provided in the Indicators of Compromise section:

Domain	Creation Date	Registrant	Registrar	Org Mimicked	Org Country	Domain Mimicked	Industry
microfocus-official[.]com	2016-10-28	Andrey Arseniev	PDR Ltd. d/b/a	Micro Focus International	United Kingdom	microfocus.com	Software Development

perrigointernational[.]com	2016-10-28	Andrey Arseniev	PDR Ltd. d/b/a	Perrigo Company plc	United States	perrigo.com	Healthcare
ornuafood[.]com	2016-10-28	Andrey Arseniev	PDR Ltd. d/b/a	Ornua Food	Ireland	ornua.com	Food Production
esb-energy-int[.]com	2016-10-27	Dresde Nore	PDR Ltd. d/b/a	Electricity Supply Board	Ireland	esb.ie	Utilities & Electric
fda-gov[.]com	2016-12-09	Smolin Sergei	PDR Ltd. d/b/a	US Food and Drug Administration (FDA)	United States	fda.gov	Government
treasury-government[.]com	2016-12-09	Smolin Sergei	PDR Ltd. d/b/a	US Department of the Treasury	United States	treasury.gov	Government
bentley-systems-ltd[.]com	2016-10-27	Dresde Nore	PDR Ltd. d/b/a	Bentley Systems	United States	bentley.com	Software Development
zynga-ltd[.]com	2016-10-27	Dresde Nore	PDR Ltd. d/b/a	Zynga	United States	zynga.com	Software Development
syngenta-usa[.]com (*)	2016-10-27	Dresde Nore	PDR Ltd. d/b/a	Syngenta	Switzerland	syngenta-us.com	Agriculture/BioTech
ai0ha[.]com	2016-11-29	Garry Torp	PDR Ltd. d/b/a	Aloha, Inc.	United States	aloha.com	Nutritional Supplements
iris-woridwide[.]com	2016-11-29	Garry Torp	PDR Ltd. d/b/a	iris Worldwide	United Kingdom	iris-worldwide.com	Marketing/Public Relations
strideindustrialusa[.]com	2015-12-21	Andrew Zavok	PDR Ltd. d/b/a	Stride Industrial Group Ltd	United Kingdom	strideindustrialgroup.com	Manufacturing
waldorfs-astoria[.]com	2016-12-11	Fred Hesl	PDR Ltd. d/b/a	Waldorf-Astoria	United States	waldorf-astoria.com	Hospitality
atlantis-bahamas[.]com	2016-12-11	Fred Hesl	PDR Ltd. d/b/a	Atlantis Bahamas	Bahamas	atlantisbahamas.com	Hospitality
sizzier[.]com	2016-12-01	Egor Danilkin	PDR Ltd. d/b/a	Sizzler Family Restaurants	United States	sizzler.com	Restaurant Chain
taskretaiitechnology[.]com	2016-12-01	Egor Danilkin	PDR Ltd. d/b/a	Task Retail Technology	Australia	taskretailtechnology.com	Software Development
dhl-service-au[.]com	2016-09-27	Remin Vladmiri	PDR Ltd. d/b/a	DHL Australia	Australia	dhl.com.au	Logistics
prsnewwire[.]com	2016-08-30	Remin Vladmiri	PDR Ltd. d/b/a	PR Newswire	United States	prnewswire.com	Marketing/Public Relations

(*) Legitimate organization reclaimed the mimicked/spoofed domain.

Once the malicious domain had been registered, the group would point it to one of the following IP addresses:

Domain Mirroring

The Threat Actor would then use the TelePort Pro or TelePort Ultra software to mirror the content of the legitimate organization's web site to the newly registered domain. While in the majority of cases the TelePort Pro software would "flawlessly" mirror the web sites, if the web page contains links to external pages which are outside the scope of the TelePort site mirroring configuration, the software will rewrite some of the links in the mirrored HTML files as follows:

Traces of TelePort Ultra seen on irisworidwide[.]com domain:

<img src="icon-twitter.png" tppabs="http://www.iris-worldwide.com/media/1239/icon-twitter.png" alt="Twitter">

Traces of TelePort Pro seen on prsnewwire[.]com domain:

<a href="javascript:if(confirm(%27http://www.omniture.com/ \n\nThis file was not retrieved by Teleport Pro, because it is addressed on a domain or path outside the boundaries set for its Starting Address. \n\nDo you want to open it from the server? %27))window.location=%27http://www.omniture.com/%27" tppabs="http://www.omniture.com/" title="Web Analytics">

Malware Delivery

We were able to identify and confirm at least two separate instances where above domains were used to serve up malicious Office documents:

The malware document "order.docx" is a stage 1 binary which, when opened by the end user, will download a stage 2 binary through the embedded macros in the malicious Office document. TrustWave recently did a great write up entitled "New Carbanak / Anunak Attack Methodology", which provides additional details regarding the malware used in that campaign, as well as an overview of C2 communications and actor TTPs. Based on correlation of TTP's and infrastructure, we are fairly confident that the TelePort Crew is closely affiliated with, or is in fact the Carbanak Threat Actor. We also believe the "Digital Plagiarist" campaign is associated with, or an evolution of, the campaign described in the recent TrustWave report.

Once the domains were properly mirrored and outfitted with malware, the TelePort Crew would craft spearphishing emails to their targets in order to lure them to download and open malicious Office documents hosted on one of the above domains. We have been able to observe at least one reported instance of such a spearphishing email related to the "Digital Plagiarist" campaign.

```
barry_frith@shoneys.com -> "mailto:sizzier_company@yahoo.com"

From: barry_frith@shoneys.com
Sent: Wednesday, December 14, 2016 10:33 AM
To: R_bgt, Briargate 0186
Subject: catering

Hello,

My name is George Thon and I'm an Project Manager with Sizzier Ltd.

We have composed a list of services we require and interested in.

Enclosed link contains all catering informatiom - http://www.sizzier.com/docs/order.docx

Click on edit anyway at the top of the page and than double click to unlock content

Sincerely,
George Thon
Sizzier Ltd.
```

Campaign and Infrastructure Clean Up

At the time of this writing, at least one of the malicious documents is still being served on one of the above listed domains. While all of the above listed domains are still active, only a few are still serving up mirrored content. When we started investigating this threat actor a few months ago, we were able to observe that almost all of the above listed domains were, at one time, serving up mirrored page content.

Based on all elements of our research, we believe the TelePort Crew threat actor will remove malicious and non-malicious content once successful execution of the malware on the target has been achieved. At the same time, our analysis leads us to suggest that the TelePort Crew may also delete or rename malicious content when the Threat Actor believes their operation has been compromised.

Targeted Industry / Organizations Interrelations

As we started investigating the Teleport Crew threat actor and the "Digital Plagiarist" campaign, it became apparent fairly quickly that the group has spent a considerable effort in understanding and mapping out affinities and business/customer relationships between their targets and the domains they would register.

A good example of that is the relationship between Sizzler Family Restaurants (TelePort Crew registered "sizzier[.]com") and Task Retail Technology (TelePort Crew registered "taskretaiitechnology[.]com"):

- Sizzler Family Restaurants is a restaurant chain operating in the United States and abroad (including Australia).
- Task Retail Technology is a software development company based in Australia, who develop the xchangexec Enterprise Point-of-Sale (POS) software.
- The Task Retail Technology web site lists Sizzler as one of their customers.

Another, yet less obvious example, is that of the "relationship" between Perrigo (TelePort Crew registered "perrigointernational[.]com") and Syngenta (TelePort Crew registered "syngenta-usa[.]com"):

- Perrigo is a US based Pharmaceutical Company.
- Syngenta is a Swiss Agribusiness/BioTech firm, with offices in the United States.
- Based on multiple news reports [1] [2] [3] [4], both firms have seen similar investor profiles and were also both linked to Merger & Acquisition activity over the past year.

In a potentially more sinister, and entirely speculative twist, there may be a relationship between TrustWave and iris Worldwide Marketing (TelePort Crew registered "iris-woridwide[.]com"):

- iris Worldwide is marketing company responsible for marketing of some of the world's biggest brands.
- TrustWave is a security company who recently published an article regarding the Carbanak / Anunak Threat Actor and their new Attack Methodology.
- Apparently, iris Worlwide was responsible for a marketing campaign around TrustWave's Global Security Report.

Attribution

The tr1adx team initially started tracking this Threat Actor under the codename "TelePort Crew" as a result of some of their TTP's. As we were delving deeper into the group's activities, we were seeing increasing overlap with TTP's and infrastructure associated with the Carbanak / Anunak threat actor, which was confirmed as we compared notes with the information in the TrustWave article, entitled "New Carbanak / Anunak Attack Methodology", published in November 2016.

Several elements strongly suggest TelePort Crew and Carbanak/Anunak may be one and the same threat actor:

- tr1adx's investigation, as well as the TrustWave investigation, point to a single IP address where the registered domains were hosted (192.99.14.211)
- tr1adx's investigation revealed that two domains we had been tracking (dhl-service-au[.]com and prsnewwire[.]com) were registered by a Registrant Name purporting to be "Remin Vladmiri". The same individual also registered "park-travels[.]com", which has been associated with the Carbanak/Anunak threat actor.
- The malware used in the "Digital Plagiarist" campaign appears to closely resemble that attributed to the Carbanak/Anunak threat actor, in terms of malware delivery, malware URL path, and behavior.

Disclaimer

The tr1adx team believes it is important to note that while we have seen this threat actor register domains similar in nature to domains belonging to legitimate organizations, we are in no way suggesting that these legitimate organizations or its customers were a direct target for the TelePort Crew threat actor. We do believe the group has leveraged the reputation and legitimacy of these organizations to give more credit to the "Digital Plagiarist" campaign, in turn potentially yielding a higher rate of success for compromising the group's victims.

Indicators of Compromise

Indicators of Compromise (IOCs): Domains (25+) - Summary Table

- microfocus-official[.]com
- perrigointernational[.]com
- ornuafood[.]com
- esb-energy-int[.]com
- fda-gov[.]com
- treasury-government[.]com
- bentley-systems-ltd[.]com
- zynga-ltd[.]com
- syngenta-usa[.]com
- ai0ha[.]com
- iris-woridwide[.]com
- strideindustrialusa[.]com
- waldorfs-astoria[.]com
- atlantis-bahamas[.]com
- sizzier[.]com
- taskretaiitechnology[.]com
- dhl-service-au[.]com
- prsnewwire[.]com
- google-ssls[.]com
- google-stel[.]com
- google3-ssl[.]com
- google4-ssl[.]com
- ssl-googles4[.]com
- google2-ssl[.]com
- google5-ssl[.]com
- ssl-googlesr5[.]com
- bols-googls[.]com

Indicators of Compromise (IOCs): IP Addresses - Summary Table

- 192.99.14.211
- 31.41.41.41
- 144.76.61.231

Indicators of Compromise (IOCs): File Hashes - Summary Table

- order.docx
  - MD5: 950afc52444e3b23a4923ab07c1e7d87
  - SHA1: 1827a7daa98c127af11318eebe23ec367f9146c9
- order.docx
  - MD5: ae8404ad422e92b1be7561c418c35fb7
  - SHA1: 400f02249ba29a19ad261373e6ff3488646e95fb

Indicators of Compromise (IOCs) [Downloadable Files]:

If a log search for any of these Indicators of Compromise returns positive hits, we recommend you initiate appropriate cyber investigative processes immediately and engage Law Enforcement where appropriate.