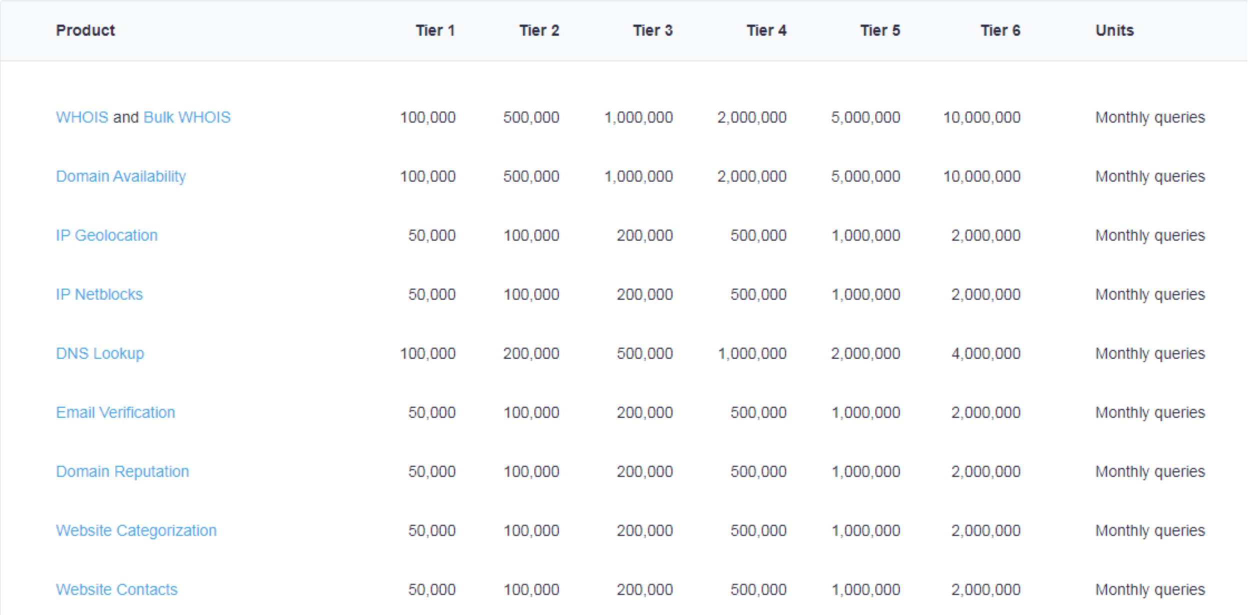
00. Person on U.S Secret Service's Most Wanted Cybercriminals List and U.S Sanctions List Runs a Profitable Managed Android Malware Enterprise - An OSINT Analysis

01. Introduction to WHOIS XML API

WhoisXML API is one of the Web's and the security industry's primary destinations for threat intelligence and cybercrime research including OSINT type of domain, IP, and current and historical WHOIS data records with billions of domain IP and WHOIS records within WhoisXML API's database where novice and experienced cybercrime researchers threat intelligence analysts including OSINT experts and analysts should consider adopting WhoisXML API's in their arsenal of OSINT tools and public database repositories and databases largely considering the tool as their primary information source and threat intelligence gathering tool and publicly accessible database in terms of using it in their current and ongoing OSINT and cybercrime including threat intelligence type of investigations.

02. How to get a proper account

Cybercrime researchers and threat intelligence analysts interested in obtaining access to one of the Web's and the industry's most comprehensive and in-depth data set of real-time and historical domain IP and WHOIS information should grab an account from the following URL - https://main.whoisxmlapi.com/signup for the purpose of beginning their OSINT and cybercrime research including their threat hunting and threat intelligence gathering process.

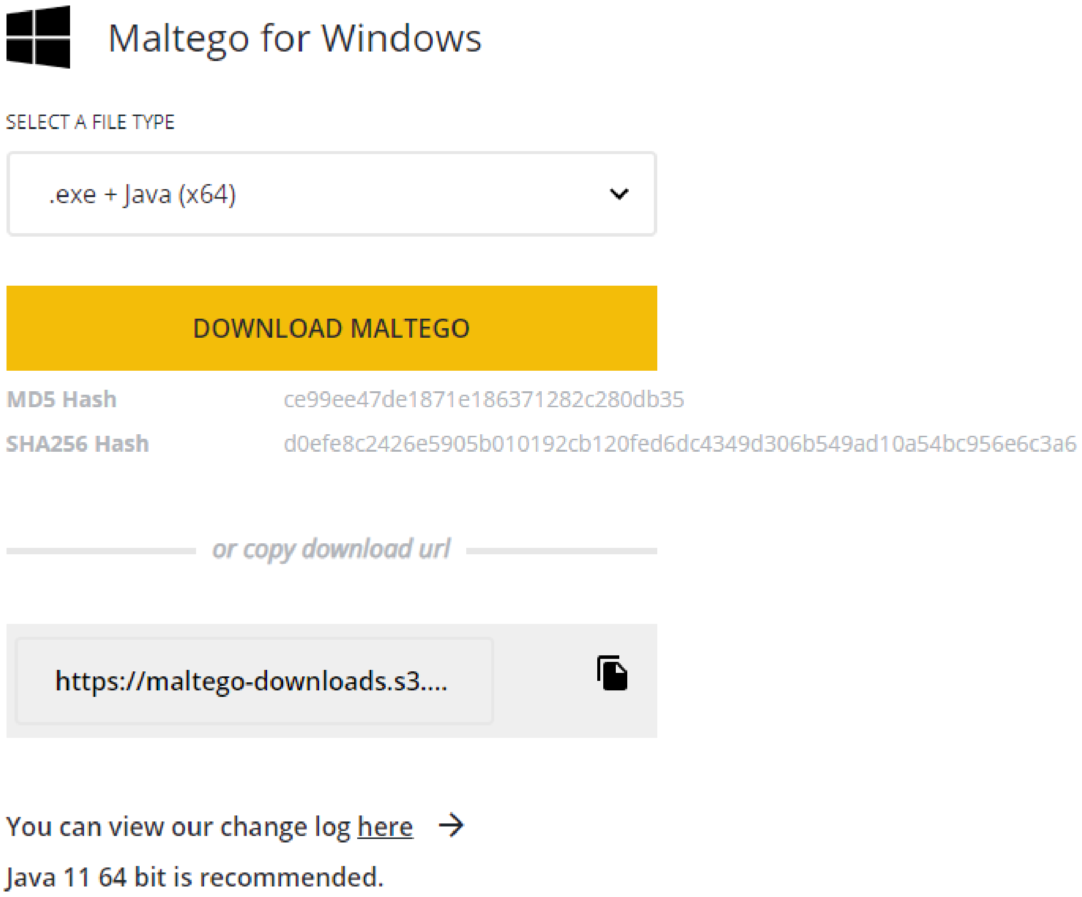


Product	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5	Tier 6	Units
WHOIS and Bulk WHOIS	100,000	500,000	1,000,000	2,000,000	5,000,000	10,000,000	Monthly queries
Domain Availability	100,000	500,000	1,000,000	2,000,000	5,000,000	10,000,000	Monthly queries
IP Geolocation	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
IP Netblocks	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
DNS Lookup	100,000	200,000	500,000	1,000,000	2,000,000	4,000,000	Monthly queries
Email Verification	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
Domain Reputation	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
Website Categorization	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
Website Contacts	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries

Sample WhoisXML API Pricing Plans Web Site

03. How to install Maltego

For the purpose of this case study we'll use the popular OSINT gathering and enrichment tool Maltego which you can grab from the following URL - https://www.maltego.com/downloads/ on your way to begin using and utilizing WhoisXML API's advanced domain IP and historical and current WHOIS information and one of the Web's and the industry's most comprehensive and in-depth database.



Maltego for Windows

SELECT A FILE TYPE

.exe + Java (x64)

MD5 Hash ce99ee47de1871e186371282c280db35

SHA256 Hash d0efe8c2426e5905b010192cb120fed6dc4349d306b549ad10a54bc956e6c3a6

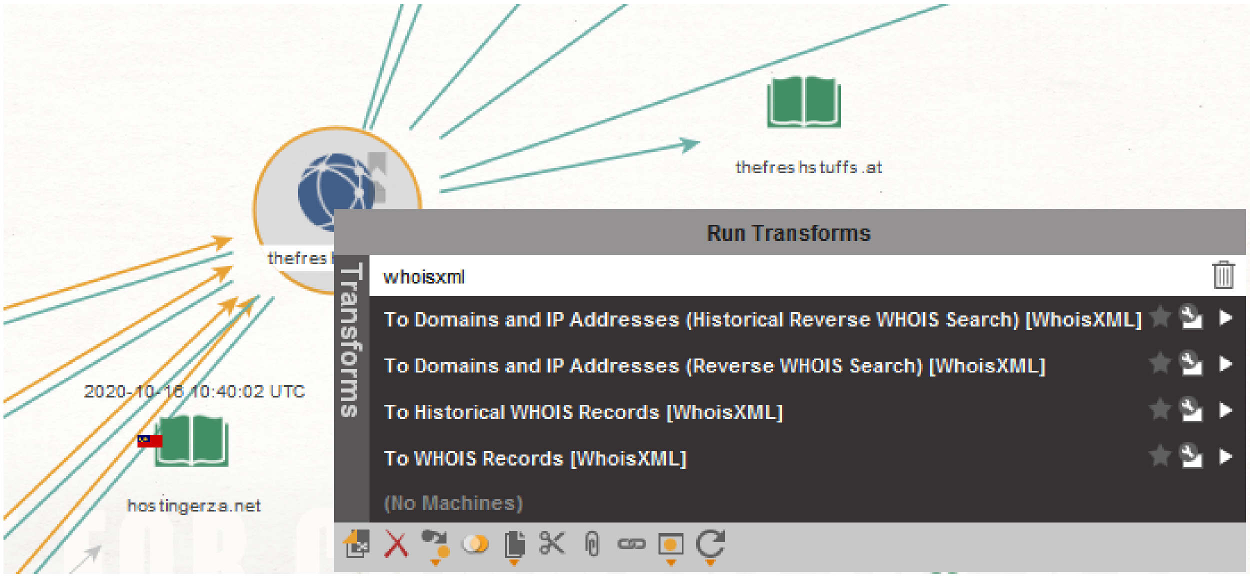
https://maltego-downloads.s3....

You can view our change log here →

Java 11 64 bit is recommended.

Sample Maltego Download Web Site

04. How to use the WHOIS XML API Maltego Integration

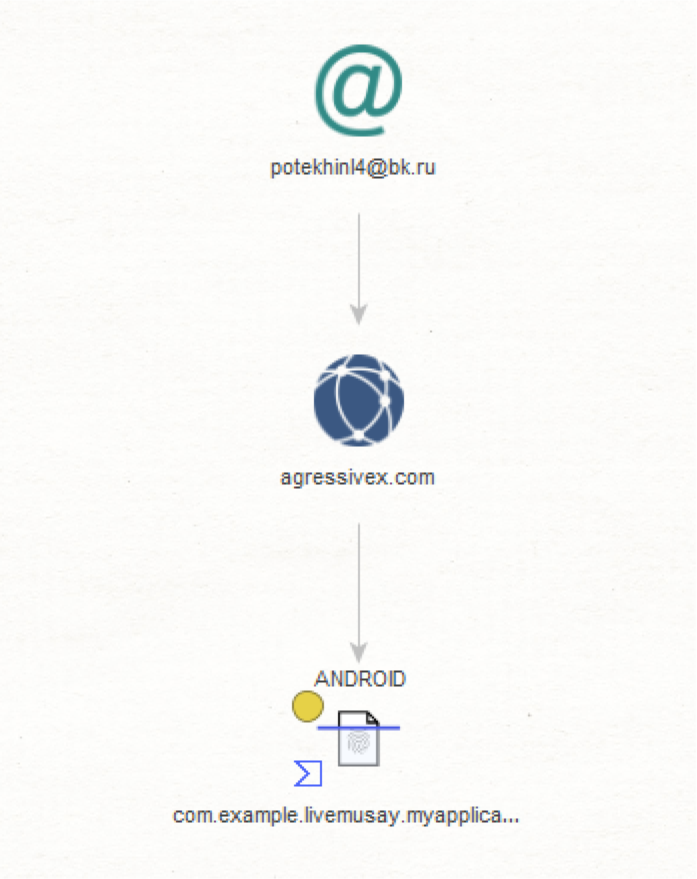

thefreshstuffs.at
thefres
2020-10-16 10:40:02 UTC
hostingerza.net
Run Transforms
Transforms
whoisxml
To Domains and IP Addresses (Historical Reverse WHOIS Search) [WhoisXML]
To Domains and IP Addresses (Reverse WHOIS Search) [WhoisXML]
To Historical WHOIS Records [WhoisXML]
To WHOIS Records [WhoisXML]
(No Machines)

Before using Maltego users should follow the instructions and grab a proper WhoisXML API account which they can later one use for the actual research and OSINT research and analysis including the actual enrichment process.

05. The Case Study

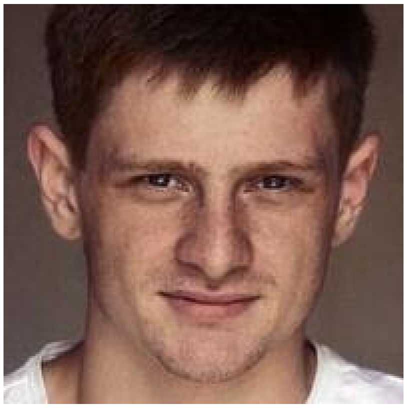
We've recently decided to take a look at the U.S Secret Service's Most Wanted Cybercriminals list which we closely monitor and track for new developers for the purpose of using basic OSINT techniques on our way to attempt to track down and collect and present personally identifiable information including technical details behind one of the U.S Secret Service's Most Wanted cybercriminals and we succeeded in doing that by finding out and providing additional information on one of their Web properties which is basically a managed Android malware enterprise.

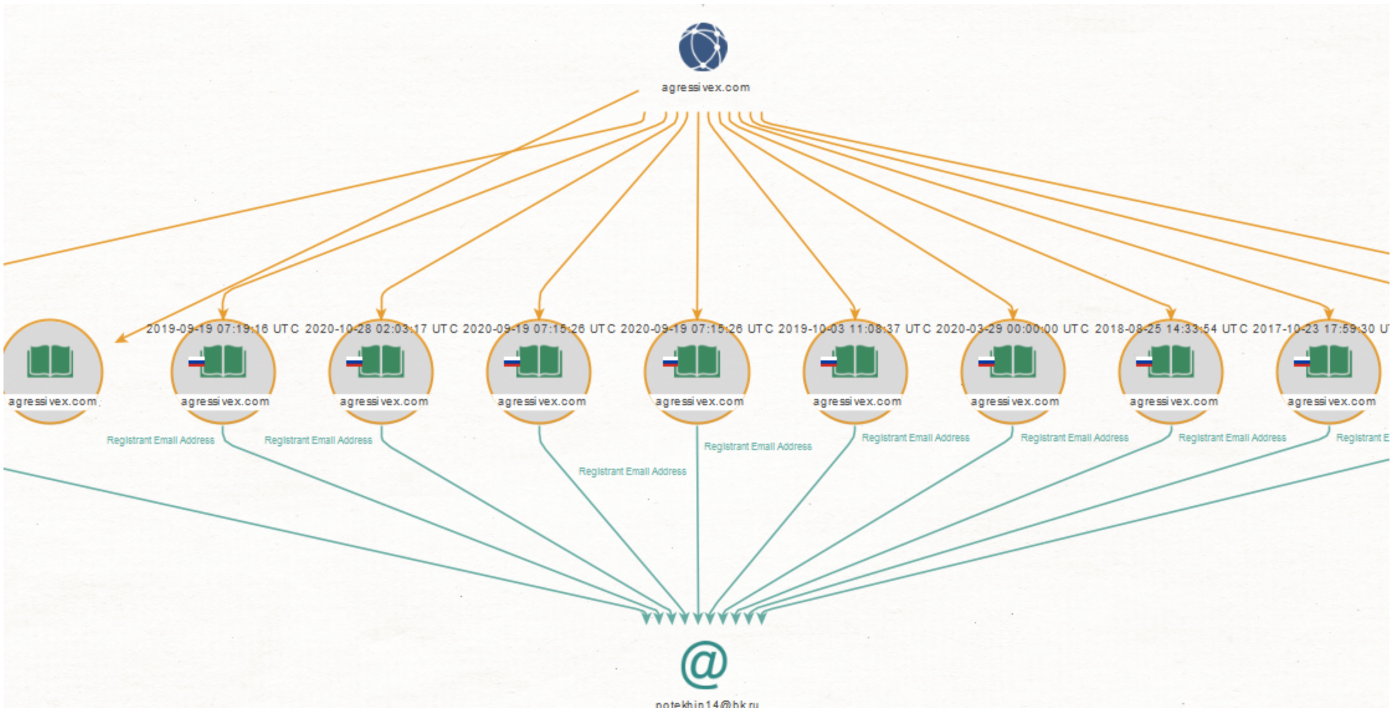
In this post we'll offer practical and technical cyber attack attribution detail on Danil Potekhin who is on the U.S Secret Service Most Wanted Cybercriminals list in terms of the online infrastructure he's currently running with the idea to assist U.S Law Enforcement on its way to track down and prosecute the cybercriminals behind these campaigns.



Sample web site he's currently running which is basically a managed Android malware botnet enterprise:
hxxp://agressivex.com

Sample personal email which we found out using OSINT techniques and used for the purpose of this case study:
potekhinl4@bk.ru





We’ll continue monitoring the campaign and post updates as soon as new developments take place.