

## 00. Person on the U.S Secret Service Most Wanted Cybercriminals Identified Runs a Black Energy DDoS Botnet - 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

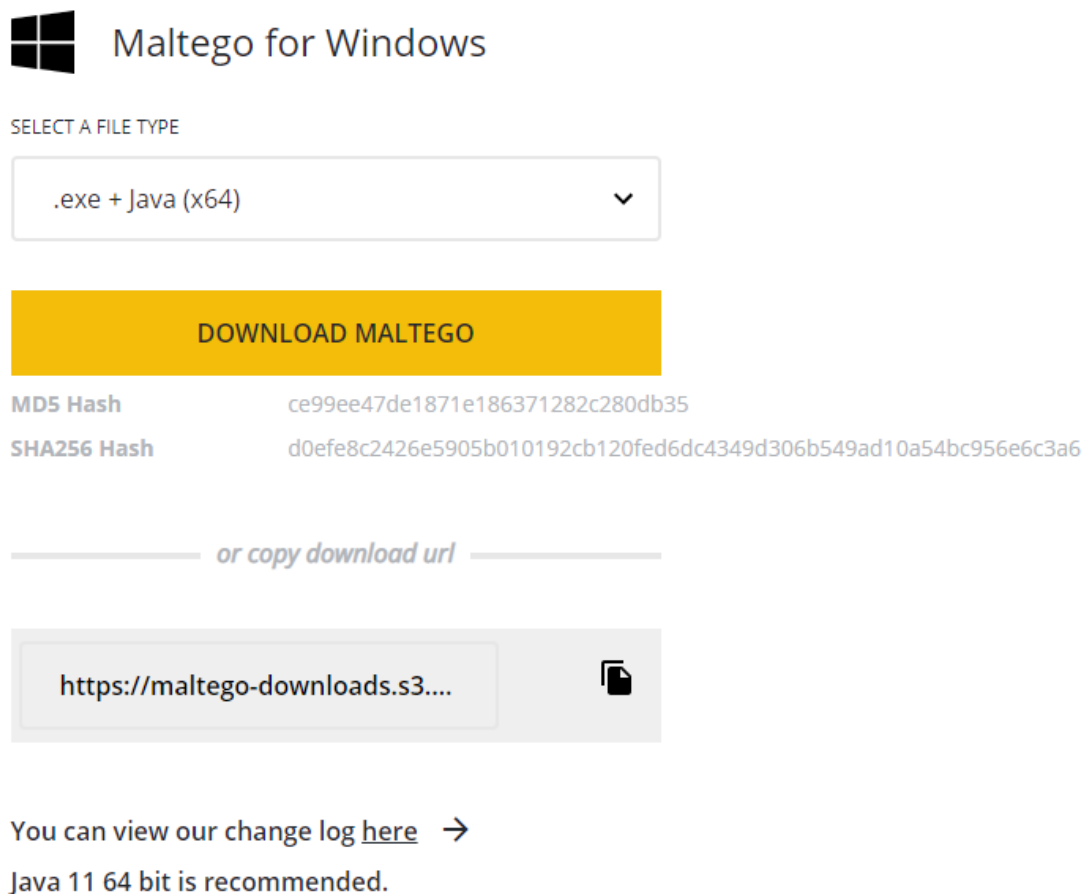
Cybercrime researchers and threat intelligence analysts interested in obtaining access to one of the Web's and the industry's most comprehensive and in-depth data set of real-time and historical domain IP and WHOIS information should grab an account from the following URL - <https://main.whoisxmlapi.com/signup> 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
<a href="#">WHOIS and Bulk WHOIS</a>	100,000	500,000	1,000,000	2,000,000	5,000,000	10,000,000	Monthly queries
<a href="#">Domain Availability</a>	100,000	500,000	1,000,000	2,000,000	5,000,000	10,000,000	Monthly queries
<a href="#">IP Geolocation</a>	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
<a href="#">IP Netblocks</a>	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
<a href="#">DNS Lookup</a>	100,000	200,000	500,000	1,000,000	2,000,000	4,000,000	Monthly queries
<a href="#">Email Verification</a>	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
<a href="#">Domain Reputation</a>	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
<a href="#">Website Categorization</a>	50,000	100,000	200,000	500,000	1,000,000	2,000,000	Monthly queries
<a href="#">Website Contacts</a>	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) ▼

**DOWNLOAD MALTEGO**

**MD5 Hash** ce99ee47de1871e186371282c280db35

**SHA256 Hash** d0efe8c2426e5905b010192cb120fed6dc4349d306b549ad10a54bc956e6c3a6

or copy download url

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

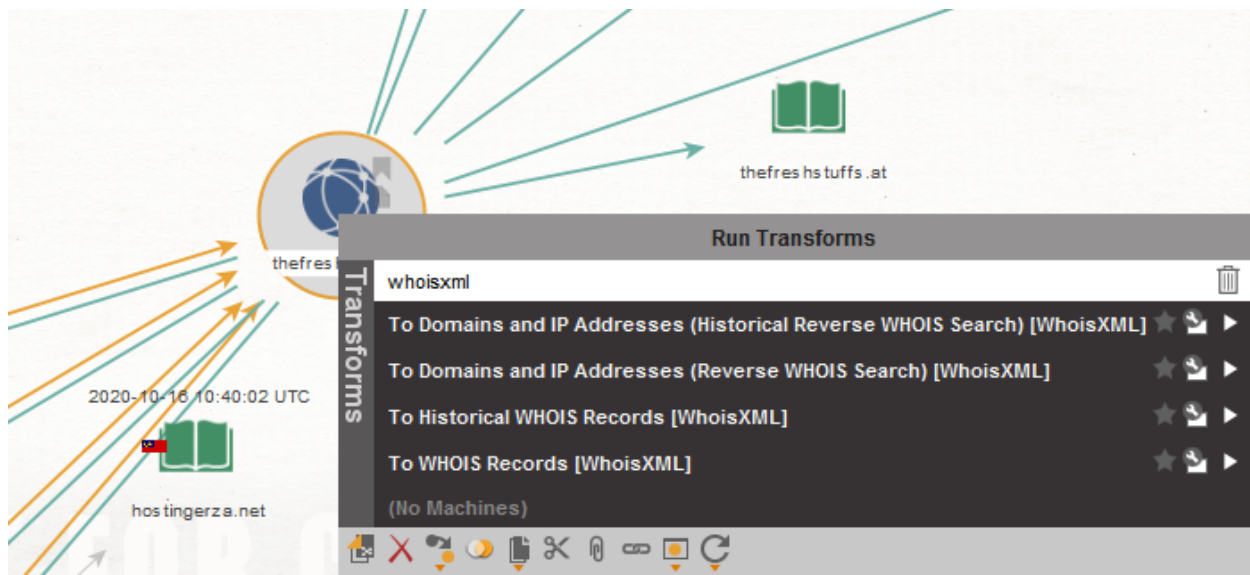
You can view our change log [here](#) →

Java 11 64 bit is recommended.

*Sample Maltego Download Web Site*

#### **04. How to use the WHOIS XML API Maltego Integration**

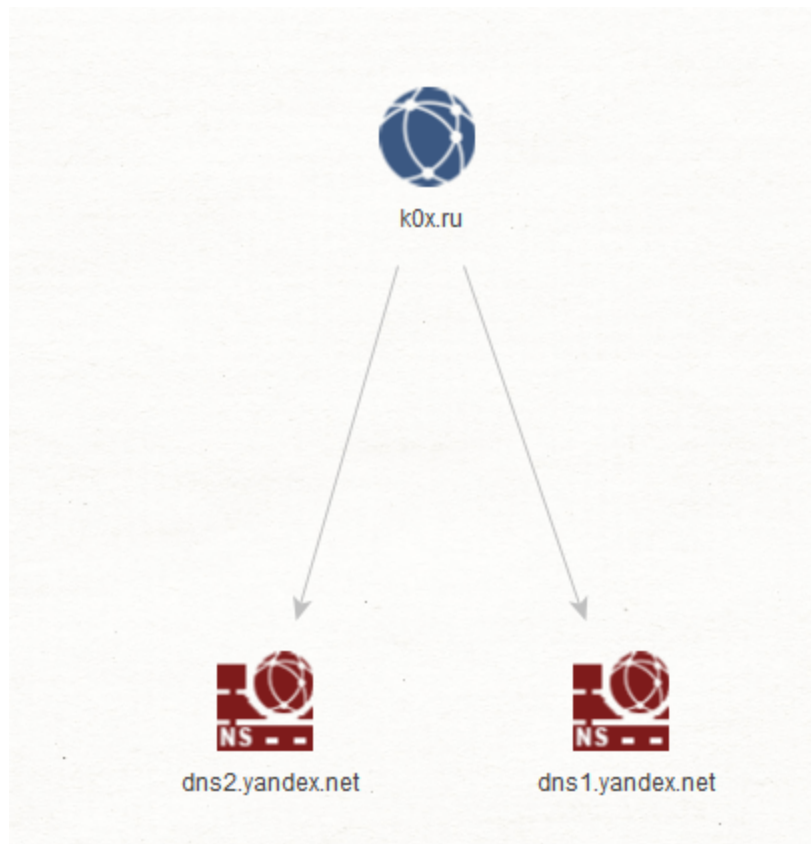
Before using Maltego users should follow the instructions and grab a proper WhoisXML API account which they can later use for the actual research and OSINT research and analysis including the actual enrichment process.



## 05. The Case Study

We've decided to dig a little bit deeper inside the U.S Secret Service Most Wanted Cybercriminals list and we've managed to find personally identifiable information on one of the most wanted cybercriminals Oleksandr Vitalyevich Ieremenko and managed to connect one of his major Web properties with a currently active BlackEnergy DDoS botnet for hire service and we've decided to provide actionable threat intelligence and personally identifiable information on its Internet-connected infrastructure with the idea to assist U.S Law Enforcement on its way to track down and prosecute the cybercriminals behind these campaigns.

In this analysis we'll provide personally identifiable information on Oleksandr Vitalyevich Ieremenko and one of his Web properties which is basically a BlackEnergy DDoS for hire botnet C&C server domain with the idea to assist the security community and U.S Law Enforcement on its way to track down and prosecute the cybercriminals behind these campaigns.



```
POST /black_energy_31337_/stat.php
HTTP/1.1
Content-Type: application/x-www-
form-urlencoded
User-Agent: Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1; SV1; .NET
CLR 1.1.4322)
Host: k0x.ru
Content-Length: 44
Cache-Control: no-cache

id=xCASPER-5D225B80_
E8401F1D&build_id=6DE983
```

**Personally Identifiable Information:**

**Primary Web site URL:** <http://k0x.ru>

**ICQ:** 123424

Personal Email: [lamarez@mail.ru](mailto:lamarez@mail.ru); [uaxakep@gmail.com](mailto:uaxakep@gmail.com)



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