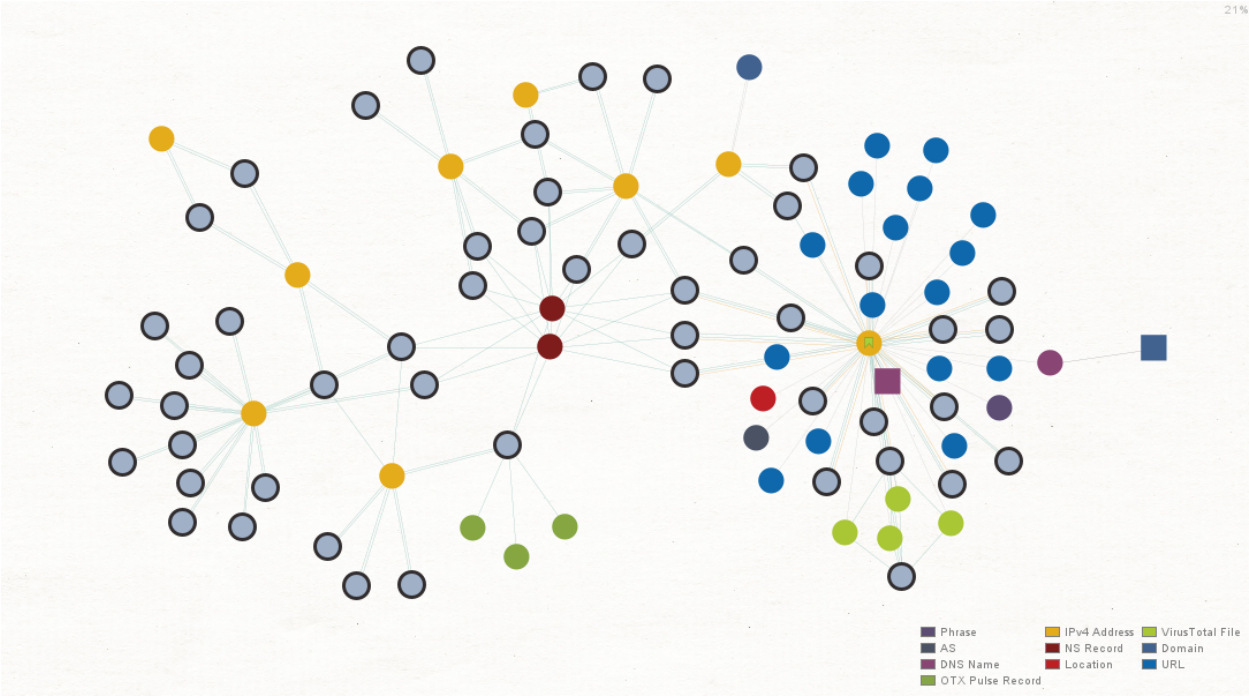
00. Exposing "Void Balaur" Internet-Connected Infrastructure - From Typosquatting Google's GMail for Spear Phishing Campaigns to a Vast and Vibrant Online Infrastructure for Launching and Orchestrating Fraudulent Attacks Based in Latvia - An OSINT Analysis



In our most recent case study we've decided to use WhoisXML API's vast real-time and historical WHOIS database where we've uncovered a recent development in the "Void Balaur" online malicious cybercrime gang syndicate spear-phishing launching online organization which in reality was the actual registration of yet another typostuatted spear-phishing domain impersonating Google's GMail where we've decided to dig a little bit further by properly researching the actual infrastructure behind the "Void Balaur" cybercrime syndicate and coming up with a Maltego case study on the topic.

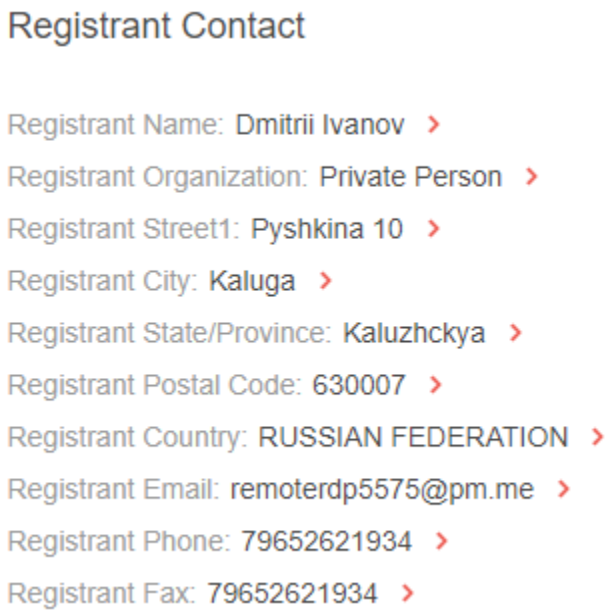
In this article we'll take a deeper look inside the "Void Balaur" online infrastructure and provide actionable and relevant intelligence on its whereabouts including the dig a little bit deeper in the context of providing additional actionable intelligence and information based on the actual domain name registrant email address accounts that we've uncovered by using WhoisXML API's vast and in-depth real-time and historical WHOIS database.

The majority of typosquatted and ready to be used for spear-phishing campaigns domains that impersonate Google's GMail seem to be registered using a single email address account which we uncovered as part of the group's online infrastructure management team.

Sample entry in our Registrant Monitor for the actual cybercriminal's domain registration personal email address account where we use our technology to monitor him for new

domain registrations which we believe will be definitely malicious or will at least offer us a clue as to their real whereabouts and intentions online:

Sample WHOIS output using WhoisXML API's WHOIS Database indicating that the group operates out of Russia where we could also easily conclude and actually produce a Current WHOIS or Historical Reverse WHOIS record for the domain's registrant name and actually once again observe related typosquatted domain registrations which impersonate Google's GMail service in possible spear-phishing campaigns:



The following is a list of all the currently active typosquatted and ready to be used for spear-phishing campaigns domain that impersonate Google GMail and are registered using the same domain registrant email address account (**remoterdp5575@pm[.]me**):

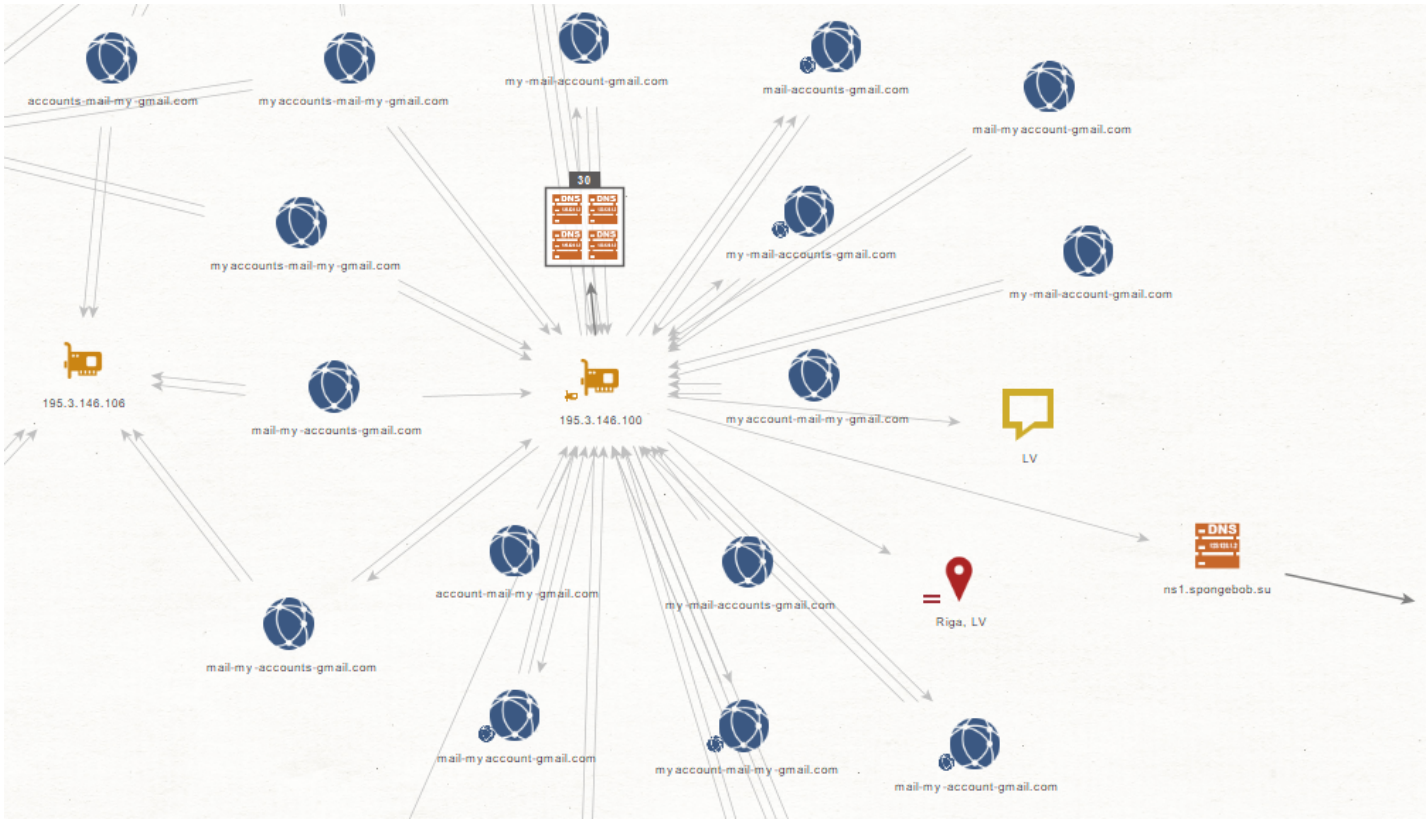
my-mail-account-yahoo[.]com
my-oauth-account-gmail[.]com
my-signin-accounts-gmail[.]com
accounts-mail-my-gmail[.]com
account-mail-my-gmail[.]com
my-signin-account-gmail[.]com
accounts-my-mail-gmail[.]com
security-myaccounts-goglemail[.]com
security-my-goglemail[.]com
myaccounts-mail-my-gmail[.]com
myaccount-mail-my-gmail[.]com
mail-yahoo-myaccounts[.]com
my-mail-account-gmail[.]com

security-myaccount-goglemail[.]com
my-account-security-goglemail[.]com
mail-yahoo-myaccount[.]com
my-mail-accounts-gmail[.]com
mail-my-accounts-gmail[.]com
accounts-mail-goglemail[.]com
myaccount-mail-goglemail[.]com
mail-myaccount-yahoo[.]com
mail-myaccounts-gmail[.]com
mail-myaccount-gmail[.]com
mail-my-account-gmail[.]com
security-accounts-goglemail[.]com
my-mail-account-yahoo[.]com
my-oauth-account-gmail[.]com
my-signin-accounts-gmail[.]com
accounts-mail-my-gmail[.]com
account-mail-my-gmail[.]com
my-signin-account-gmail[.]com
accounts-my-mail-gmail[.]com
security-myaccounts-goglemail[.]com
security-my-goglemail[.]com
myaccounts-mail-my-gmail[.]com
myaccount-mail-my-gmail[.]com
mail-yahoo-myaccounts[.]com
my-mail-account-gmail[.]com
security-myaccount-goglemail[.]com
my-account-security-goglemail[.]com
mail-yahoo-myaccount[.]com
my-mail-accounts-gmail[.]com
mail-my-accounts-gmail[.]com
accounts-mail-goglemail[.]com
myaccount-mail-goglemail[.]com
mail-myaccount-yahoo[.]com
mail-myaccounts-gmail[.]com
mail-myaccount-gmail[.]com
mail-my-account-gmail[.]com
security-accounts-goglemail[.]com

The following are the currently active and responding IPs for this portfolio of typosquatted domains impersonating Google's GMail for spear-phishing campaigns:

195.3.146.100
194.58.112.170
194.58.112.174

195.3.146.106
195.3.146.99
95.173.132.1
185.246.130.170
194.58.112.169
193.105.134.29



We've also uncovered the following malicious MD5s known to have phoned back to one of the same typosquatted domains impersonating Google's GMail in this campaign:

eb7a1cb3aeb342319477160583a767c4a0df303e7014b227167eeddd86ae55fe
073425128f8af930134911be25b3e7df94c1c1890d6b8b149ddbd91645a75995
9230d02930c2f2c7426b24a9783bfbd80261d152895d15767f8c0f25c21a1409
61dc17ab0d0f1e53e378ec43b5f2203b4dffd9d440b2dc48587b9312935982ee

We'll continue monitoring the campaign including the domain's registrant personal email address account for newly registered malicious and fraudulent typosquatted domains impersonating Google's GMail including possible related campaigns and will post updates as soon as new developments take place.