RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure | RiskIQ

Published: 2022-03-15 · Archived: 2026-04-05 17:27:14 UTC

The cybersecurity community has published impactful research uncovering and tracking cyberattacks against Ukrainian citizens, refugees, and armed forces. RiskIQ is leveraging our global telemetry to add to this research however we can, including shining light on new tactics and threat infrastructure and publishing as many new threat indicators as we can.

This roundup will highlight our researchers' focus on these campaigns, including analyzing phishing attacks targeting Ukrainian refugees. We'll also add insight to other threat campaigns worldwide, including malware campaigns, nation-state threat infrastructure, and Magecart digital credit card skimming, all of which can be found in the RiskIQ Threat Intelligence Portal (TIP).

A Closer Look at Campaigns Targeting Ukraine

Fraudulent Website Spoofing UNHCR for Ukrainian Refugees Seeks Bitcoin Donations: RiskIQ researchers identified a fraudulent domain (unhcr-ukraine[.]org) spoofing the UN High Commission for Refugees for Ukraine website. The attackers used HTTrack, a popular method of copying legitimate sites—often for malicious purposes. In this case, HTTrack was used to emulate the legitimate UNHCR website to trick people into "donating" Bitcoin in support of refugees.

Two QR codes were on the donation page for the fraudulent UNHCR website, generated for Binance and Ethereum. The threat actor attempted to lure users to this fraudulent website via Reddit forums. Their username, 'asetinzjr,' spammed many different Subreddits with the same post, seeking donations via the phony site.

UNC1151/GhostWriter Phishing Attacks Target Ukrainian Soldiers: RiskIQ researchers analyzed domains published by CERT-UA known to be used by UNC-1151, also known as GhostWriter, for phishing attacks against Ukrainian soldiers. They uncovered dozens more probable phishing domains tied to the group, with several still active and resolving to known IPs.

Based on overlaps in actor infrastructure, RiskIQ has also identified 38 additional historical and active domains associated with this group based on WHOIS registration. Of those 38 domains, some are still active and resolving to IP addresses in the RiskIQ PDNS database. You can read more about this campaign in Dark Reading.

Conti Ransomware Operation Leaks: The Conti ransomware operation targeted a massive data leak in late February and early March, exposing over 160,000 messages between Conti operators, source code for the ransomware, raw data files, and proof of Conti's direct connection with Trickbot malware operations. The group behind the Conti operation made public announcements supporting Russia's invasion of Ukraine, which appear to have triggered the leaks. Wizard Spider, the threat group behind Conti and Ryuk ransomware, originates from Eastern Europe and Russia and has known associations with the Russian government.

An anonymous pro-Ukrainian security researcher, likely with inside connections to the Conti group, doxxed Trickbot and Conti operation members by leaking personal information and private messages to the public. They also released a decryptor for the ransomware decoy "HermeticRansom," used against Ukrainian entities. The troves of leaked information amounting to tens of thousands of indicators, including C2 infrastructure for Conti and Trickbot operations. RiskIQ has worked to aggregate many of these from open sources and will continue to update reporting related to this leak, Conti operations, Trickbot malware, and other Wizard Spider activity.

Malware Rundown

Malware Linked to Upwork Post Seeking Content Writer for a "Newly Developed Application" Deploys DCRat: Discord's free infrastructure continues to be leveraged by threat actors to support their campaigns. Recently, RiskIQ detected a trojan file hosted on Discord's CDN that contacts multiple URLs that eventually drop DCRat, an open-source remote access tool posted to GitHub.

VirusTotal provided a second file name for this malware file, also hosted on Discord's CDN. An open-source search on this second filename revealed a job post seeking a content writer for a "newly developed application" on the freelancing website Upwork. As of February 28, the Upwork posting indicated 5-10 people had submitted proposals for the project. Via infrastructure analysis, via RiskIQ's Threat Intelligence Graph, researchers connected more than 52 files and domains to this campaign listed in the RiskIQ TIP.

Analysis of C2 Servers Related to "SunSeed" Malware Campaign: Proofpoint released an analysis of spearphishing attacks targeting European governments through a compromised email account belonging to a Ukrainian armed services member. The Principal Threat Analyst at Microsoft's Threat Intelligence Center (MSTIC), Ben Koehl, subsequently tweeted a list of IP addresses related to the reported activity. RiskIQ analysis of responses from these servers coupled with VirusTotal data yields potential additional infrastructure associated with this threat actor.

Magecart Injected URLs and C2 Domains: RiskIQ technology detected 176 Magecart and skimmer injected URLs and detected 214 unique C2 domains used by known Magecart threat actors. Note that many of these URLs are legitimate, compromised websites and that some C2 domains may be compromised but legitimate.

Stay Up to Date with the RiskIQ TIP

RiskIQ's Threat Intelligence Portal (TIP) sources hundreds of OSINT and original RiskIQ research articles enriched with indicators from the RiskIQ Global Collection Network, which spans over 2,500 networks globally and generates billions of events daily from open and closed sources. We'll continue to update the TIP with daily insights on existing and emerging campaigns and threat groups to give users more timely and actionable intelligence as current threat actors and campaigns evolve, and new ones emerge.

Be sure to sign up today so you can stay up to speed on this rapidly evolving global threat landscape.

Source: https://web.archive.org/web/20220527112908/https://www.riskiq.com/blog/labs/ukraine-malware-infrastructure/