Domains Linked to Phishing Attacks Targeting Ukraine

secureworks.com/blog/domains-linked-to-phishing-attacks-targeting-ukraine

Counter Threat Unit Research Team

Analysis of domains listed in a CERT-UA warning revealed additional domains linked to phishing attacks targeting Ukrainian government and military personnel and Polish-speaking individuals. Wednesday, March 2, 2022 *By: Counter Threat Unit Research Team*
Secureworks® Counter Threat Unit™ (CTU) researchers investigated a Computer Emergency Response Team of Ukraine (CERT-UA) warning of phishing activity posted to Facebook on February 25, 2022 (see Figure 1). CERT-UA attributed the activity to the Minsk-

based UNC1151 threat group. UNC1511 is reportedly linked to the Belarusian government and responsible for the Ghostwriter influence campaigns. As of this publication, CTU™ researchers have not validated this attribution assessment. CTU researchers attribute this activity to the MOONSCAPE threat group.

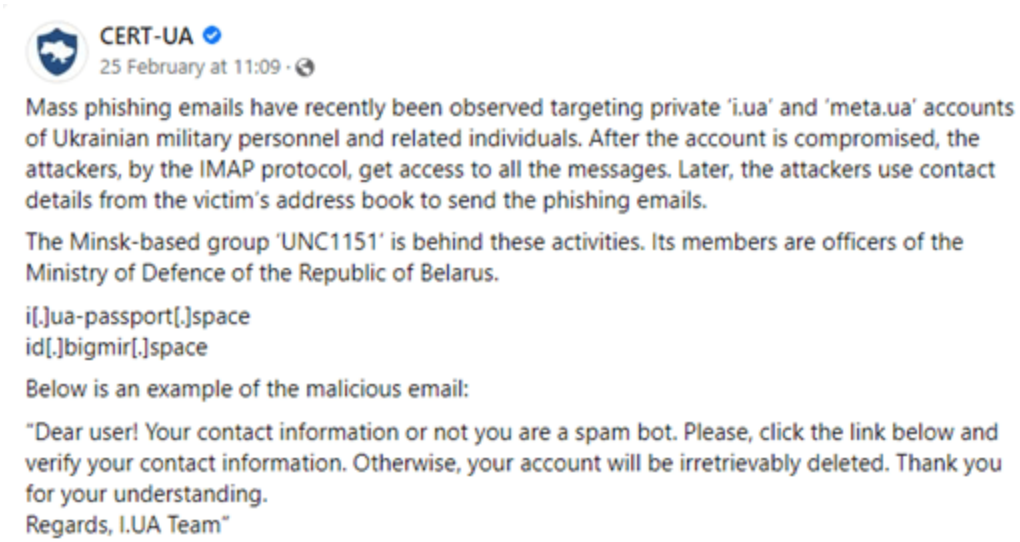

Figure 1. CERT-UA Facebook post warning of phishing attacks. (Source: Secureworks)

The rudimentary phishing message coaxes the target to use a malicious phishing link. It is possible that the phishing messages included imagery that was not included in the Facebook post.

CTU researchers analyzed the two domains listed in the Facebook post and identified seven additional domains based on WHOIS and passive DNS data. This cluster uses the '.space' top-level domain (TLD), shares a common registrant "Apolena Zorka", was registered via Public Domain Registry Ltd., and is primarily hosted behind Cloudflare infrastructure. Each of the domains aligns with a small set of common themes typical of MOONSCAPE infrastructure. Themes include information portals, email validation, cloud services, or government entities. The Apolena Zorka cluster is a mix of generic email validation and domains spoofing popular Ukrainian information services (see Figure 2). This combination suggests that the websites may have been created for Ukrainian targets, including those that prompted the CERT-UA warning.

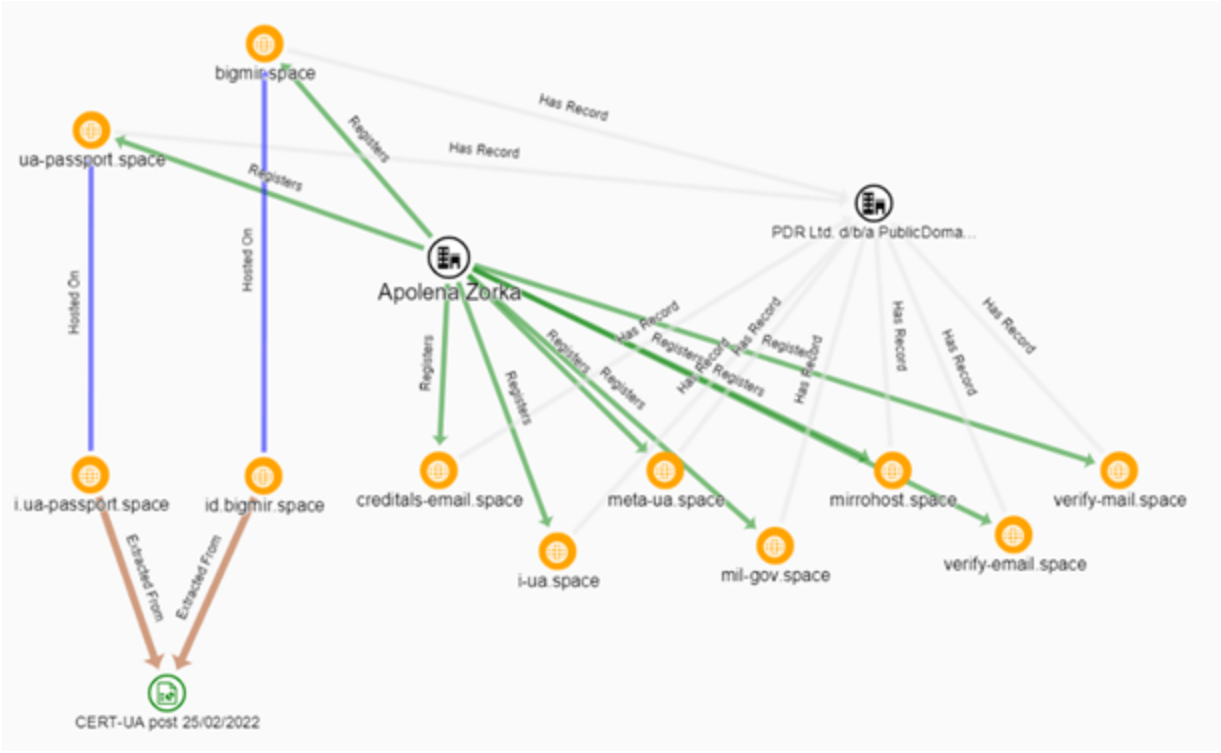

Figure 2. Apolena Zorka cluster of domains used in phishing attacks against Ukrainian targets. (Source: Secureworks)

CTU researchers identified another set of domains with similar characteristics to the Apolena Zorka cluster, although this cluster used the "Radka Dominika" registrant (see Figure 3). These domains included similar themes but used Polish words for verification (weryfikacja) and validation (walidacja) in several generic email validation-themed domains. Another identified domain (ron-mil . space) appears to spoof the legitimate domain of the Polish Ministry of National Defense (ron . mil . pl).

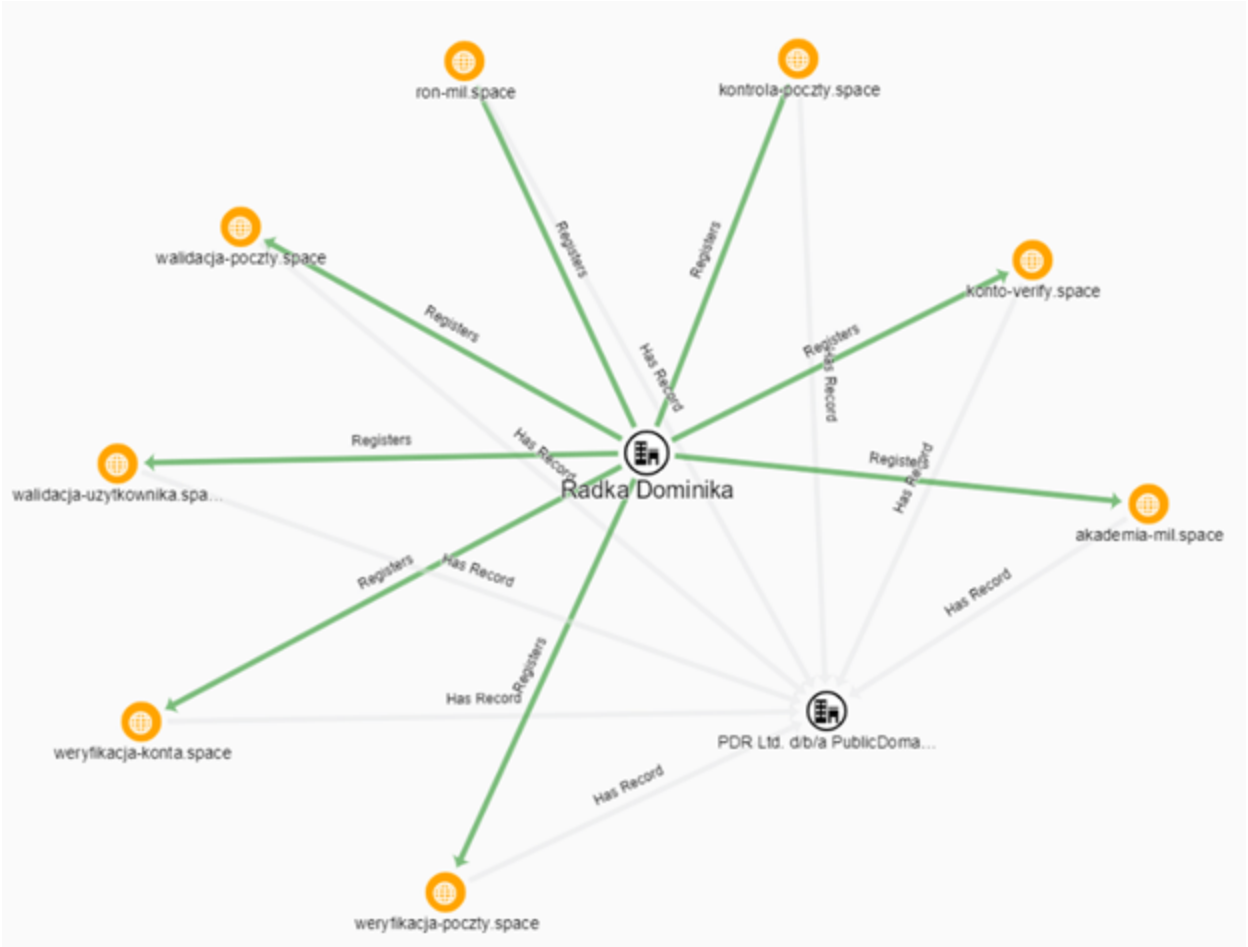

Figure 3. Radka Dominika cluster of domains likely used in phishing attacks against Polish-speaking targets. (Source: Secureworks)

When ordered by creation date, the threat actors switch between domains aligned to Ukrainian targets and domains likely aligned with Polish-speaking targets. This pattern illustrates a regular cadence of new domain creation (see Figure 4). This activity likely reflects an operational rotation involving multiple demographics they target.

domain	registrant contact org	create date
ua-passport.space	Apolena Zorka	15/12/2021
mirrohost.space	Apolena Zorka	16/12/2021
mil-gov.space	Apolena Zorka	17/12/2021
bigmir.space	Apolena Zorka	20/12/2021
kontrola-poczty.space	Radka Dominika	20/12/2021
walidacja-poczty.space	Radka Dominika	03/01/2022
weryfikacja-poczty.space	Radka Dominika	14/01/2022
konto-verify.space	Radka Dominika	25/01/2022
weryfikacja-konta.space	Radka Dominika	25/01/2022
walidacja-uzytkownika.space	Radka Dominika	26/01/2022
verify-email.space	Apolena Zorka	02/02/2022
verify-mail.space	Apolena Zorka	08/02/2022
creditals-email.space	Apolena Zorka	09/02/2022
meta-ua.space	Apolena Zorka	22/02/2022
akademia-mil.space	Radka Dominika	22/02/2022
ron-mil.space	Radka Dominika	22/02/2022
i-ua.space	Apolena Zorka	26/02/2022

Figure 4. MOONSCAPE-associated domains ordered by creation date. (Source: Secureworks)

MOONSCAPE creates new infrastructure but maintains a preference for specific keywords and reuses old infrastructure. For example, the 'verify-email . space' domain was created on February 2 and resolves to IP address 185 . 244 . 180 . 13. This IP address also hosted 'ua-passport . site', which was created on June 22, 2021. With the exception of the TLD, the 'ua-passport . site' domain is identical to the 'ua-passport . space' domain created on December 15, 2021.

MOONSCAPE has conducted phishing campaigns for years, targeting military, diplomatic, and government personnel in Eastern European NATO countries such as Poland, Lithuania, and Latvia as well as countries that border Belarus such as Ukraine. The February phishing attacks demonstrate that the group's espionage-focused activity continues and potentially contributes to intelligence collection on Ukrainian entities in support of Russia's military invasion of Ukraine that commenced on February 24, 2022.

To mitigate exposure to this malware, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 1. The domains may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
ua-passport.space	Domain name	Used in MOONSCAPE phishing attacks targeting Ukrainian government and military personnel
bigmir.space	Domain name	Used in MOONSCAPE phishing attacks targeting Ukrainian government and military personnel

Indicator	Type	Context
mirrohost.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Ukrainian government and military personnel
mil-gov.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Ukrainian government and military personnel
verify-email.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Ukrainian government and military personnel
verify-mail.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Ukrainian government and military personnel
creditals-email.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Ukrainian government and military personnel
meta-ua.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Ukrainian government and military personnel
i-ua.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Ukrainian government and military personnel
kontrola-poczty.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Polish-speaking individuals
walidacja-poczty.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Polish-speaking individuals
weryfikacja-poczty.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Polish-speaking individuals
konto-verify.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Polish-speaking individuals
weryfikacja-konta.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Polish-speaking individuals
walidacja-uzytkownika.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Polish-speaking individuals
akademia-mil.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Polish-speaking individuals
ron-mil.space	Domain name	Linked to MOONSCAPE phishing attacks targeting Polish-speaking individuals

Table 1. Indicators for this threat.