Zimperium Coverage on COLDRIVER Phishing Campaign

October 1, 2024 Santiago Rodriguez

The recently uncovered "River of Phish" campaign, attributed to the Russian threat actor COLDRIVER, targets Western and Russian civil society through sophisticated spear-phishing attacks. This campaign employs highly personalized social engineering tactics to trick targets into opening malicious PDF attachments. These PDFs contain links to phishing sites designed to steal login credentials and bypass two-factor authentication, potentially granting attackers access to sensitive information and communications of high-risk individuals and organizations.

Zimperium's advanced mobile security solution offers robust protection against this kind of campaign. By leveraging artificial intelligence and behavioral analysis, our tool can detect and block highly personalized, zero day mobile phishing attempts. Zimperium MTD scrutinizes potentially malicious PDFs and web links for telltale signs of mobile phishing and links to potentially malicious domains.

For this campaign, Zimperium detected and blocked the reported malicious PDFs.

The following table shows the chronology of the reported domains, summarizing the date for domain registration, the first report of the domain in public phishing feeds and the time difference in days (time window in which the site was potentially active as a zero day threat).

Domain	Domain Registration Date	Public Feeds Reported Date	Time Difference in Days
ithostprotocol[.]com	1/16/2024	1/18/2024	1
xsltweemat[.]org	3/14/2024	4/5/2024	21
eilatocare[.]com	4/9/2024	7/1/2024	83
egenre[.]net	5/19/2024	6/27/2024	38
esestacey[.]net	5/19/2024	8/14/2024	86
ideaspire[.]net	5/19/2024	9/27/2024	130
togochecklist[.]com	8/28/2023	8/30/2023	1
vocabpaper[.]com	3/15/2024	7/10/2024	116
matalangit[.]org	5/7/2024	8/16/2024	100
protondrive[.]me	5/7/2024	8/15/2024	100
protondrive[.]services	10/19/2023	9/12/2024	328
protondrive[.]online	2/1/2023	9/21/2024	597
service-proton[.]me	9/14/2022	8/31/2024	716

The data shows that some of the domains existed for more than 1 year before being reported. This enforces once more the importance of zero day detection tools, and not just based on lists for complete protection.

Crucially, our PDF solution offers specific safeguards against the tactics employed in this campaign. By utilizing artificial intelligence for both the analysis of PDF components and the analysis of links embedded within these files, we achieve enhanced detection in this format.

By deploying our mobile security solution, organizations can significantly mitigate the risks posed by threat actors like COLDRIVER. The system's AI capabilities provide robust protection against zero day threats, like newly created malicious sites, or previously unseen risky PDF sites.

Having a mobile security tool with capabilities for detecting zero day threats ensures the user stays ahead of evolving mobile phishing techniques, providing a critical layer of defense for high-risk individuals and organizations targeted by sophisticated cyber espionage campaigns.

Author: Santiago Rodriguez

Phishing and Data Analytics Team Leader