Iranian Exploitation Activities Continue as of November 2022

S2 Research Team ⋮⋮ 12/8/2022

Telemetry Data Suggests 107.173.231.114 Remains an Active IOC

Introduction

This blog provides a short update on Team Cymru's ongoing tracking of threat actor groups associated with Iran.

PHOSPHORUS is an Iranian threat group known to target organizations in energy, government, and technology sectors based in Europe, the Middle East, the United States, and other countries/regions. In recent reporting, PHOSPHORUS TTPs have included the likely opportunistic targeting of unpatched vulnerable systems, leveraging common exploits such as Log4J and ProxyShell.

Reports published in 2022 (for instance by the DFIR Report and Deep Instinct) have highlighted the long-term utilization of a common command and control (C2) server (**107.173.231.114 – ColoCrossing, US**), believed to be associated with PHOSPHORUS activities.

Passive DNS information historically associated **107.173.231.114** with several similarly structured domain names, for example:

- kcp53.mssync[.]one
- tcp443.mssync[.]one
- tcp443.symantecserver[.]co
- tcp.newdesk[.]top
- kcp53.newdesk[.]top
- work.newdesk[.]top

- tcp443.newdesk[.]top
- tcp443.aptmirror[.]eu
- kcp53.aptmirror[.]eu
- tcp443.msupdate[.]us
- kcp53.msupdate[.]us

Reporting by Secureworks suggested that PHOSPHORUS domains from this attack cluster were, in general, registered with Porkbun, and that some of the domains were also associated with opportunistic ransomware attacks.

However, between 30 June 2022 and 06 July 2022, the domains *aptmirror[.]eu*, *msupdate[.]us*, and *newdesk[.]top* (mentioned above) were re-registered with NameSilo. The domains were previously registered with Porkbun.

Recent observations relating to 107.173.231.114

On 14 September 2022 a joint Cybersecurity Advisory Alert (AA22-257A) was released highlighting these domains and **107.173.231.114** within the report's IOC section.

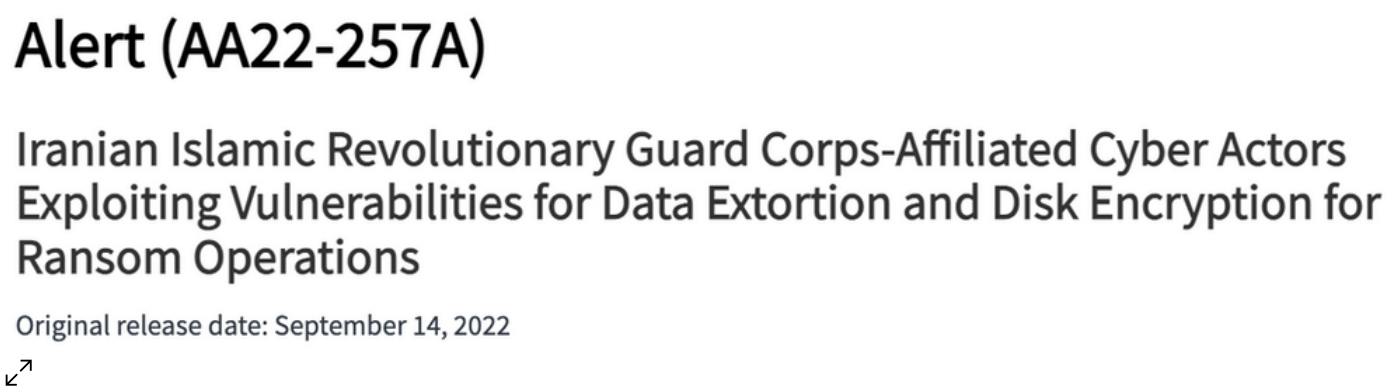

Figure 1 – CISA Alert

Having noticed the CISA alert, we conducted a review of recent network telemetry data for **107.173.231.114**, revealing that exploitation activity involving this IP likely continues.

Communications were observed between a South Asian victim and ports TCP/443 and UDP/53 of **107.173.231.114.** We assess this was likely an opportunistic compromise, based on the presence of an outdated/unpatched version of Microsoft Exchange running on the victim IP.

The activity likely indicates the malware in use relies on a hardcoded IP address vice domain resolution for ongoing C2 communications. The use of binaries with hardcoded IP addresses is a known TTP of the threat actor and was described in the previously mentioned Secureworks report.

Secondly, the victim also communicated over the same ports (TCP/443 and UDP/53) with an IP address assigned to Kaspersky. It is possible these connections equate to behavior observed in previous PHOSPHORUS samples, whereby the malware would seek to communicate with legitimate Kaspersky domains. Connections to domains such as *kcp53.kaspersky[.]com*and *tcp443.kaspersky[.]com* are potentially a means of masking malicious communications with similarly constructed domains (see the PDNS data for **107.173.231.114** above).

Reporting by Deep Instinct, referenced earlier, included these Kaspersky domains and attributed PHOSPHORUS malware with generating many connections to legitimate companies along with connections to attacker-controlled domains to confuse a network defender into categorizing the traffic as authentic traffic.

It is worth noting that the Kaspersky IP hosted both *kcp53.kaspersky[.]com* and *tcp443.kaspersky[.]com*, as well as other domains, at the time these connections were observed.

Thirdly, the victim also communicated with TCP/443 of an IP address assigned to Cloudflare. At the time of these connections, the Cloudflare IP hosted numerous domains including *api.myip[.]com*.

As noted in the previously referenced DFIR Report research, PHOSPHORUS malware was observed resolving the domain *api.myip[.]com* in the past. It is therefore possible that these connections are indicative of similar behavior – a step likely undertaken by the attackers to enrich their understanding of the victim host.

A diagram of the network activity documented above is provided below.

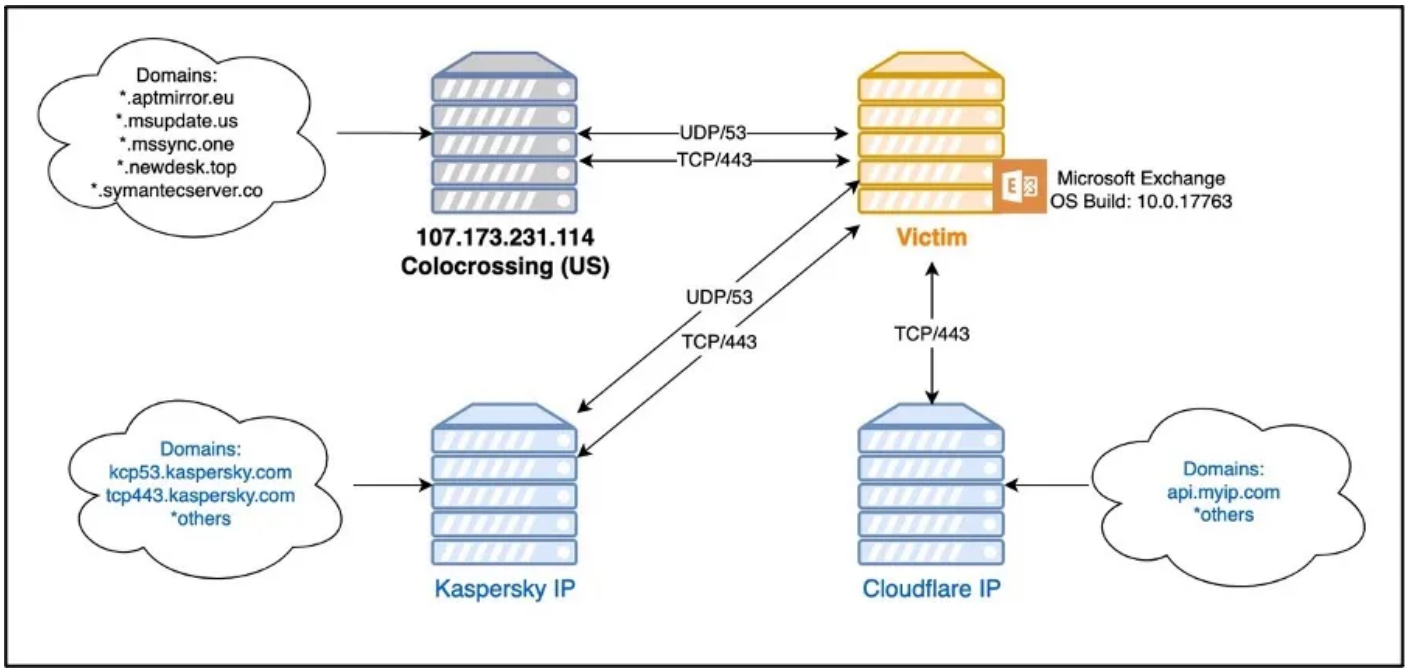

Figure 2: Network Telemetry Mapping of Victim Communications

In addition to the South Asian victim, potential victims in Africa and the Middle East were also observed communicating with both **107.173.231.114** and the Kaspersky IP over ports TCP/443 and UDP/53.

Communications with **107.173.231.114** continued as of 29 November 2022.

Recommendations

If you are concerned about assets that could be vulnerable to Log4J and ProxyShell, Team Cymru are offering a free external attack surface assessment as part of our Pure Signal Orbit evaluation experience, you can find the sign up page here.

For customers of Pure Signal Recon, add **107.173.231.114** to a query, filtering for ports TCP/443 and UDP/53.