The layered infrastructure operated by APT29

services.global.ntt/en-us/insights/blog/the-layered-infrastructure-operated-by-apt29

Threat Detection Team Security division of NTT

Reliance Securities

Reliance Securities implemented smart contact center technologies to put their customers at the heart of their operations, reducing their response times. They have also pinpointed which platform their customers prefer to communicate through.

Reliance Securities

Reliance Securities implemented smart contact center technologies to put their customers at the heart of their operations, reducing their response times. They have also pinpointed which platform their customers prefer to communicate through.

Security

By Threat Detection Team Security division of NTT

5 minute read

19 October 2021

The layered infrastructure operated by APT29

ASHRAE

ASHRAE’s new headquarters creates a blueprint for the intelligent building

ASHRAE

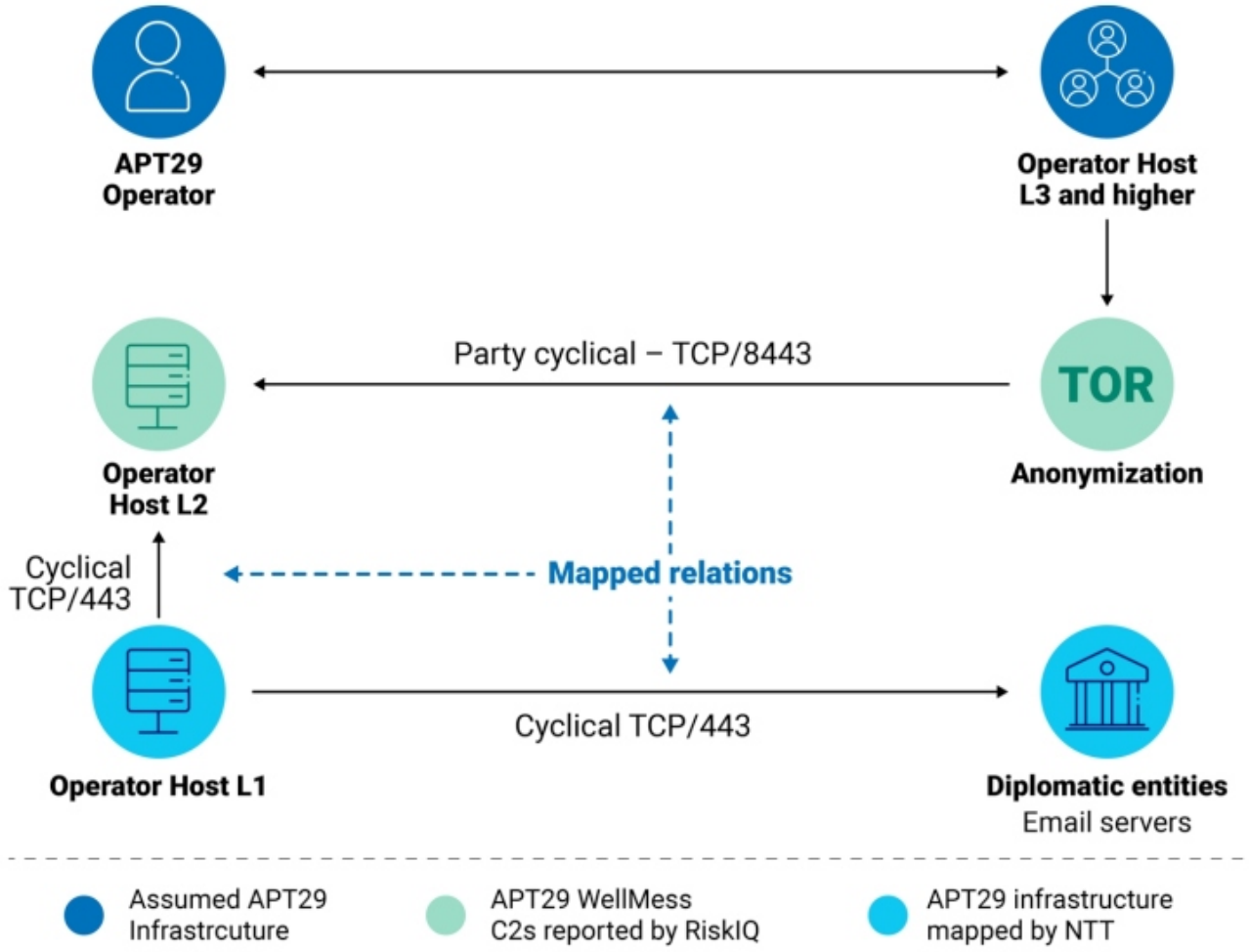
ASHRAE’s new headquarters creates a blueprint for the intelligent building

Current article

After the public reporting of APT29 activity, our analysts have mapped previously unseen layers of APT29 infrastructure.

After the public reporting of APT29 activity, our analysts have mapped previously unseen layers of APT29 infrastructure. The most recent activity included targeting email servers belonging to diplomatic entities located in South America and Northern Africa. APT29 is a threat actor commonly associated with a national intelligence service and has been widely reported to conduct espionage operations.

We initiated this research after RiskIQ reported their own research of command and control servers of the WellMess malware, operated by APT29. We discovered that some of the reported WellMess command and control servers (C2s) are used as layer 2 (L2) operator hosts (OH), while there's also a layer 1 (L1) OH in contact with the victim's email server. The targeted email servers are running open-source webmail clients that have a history of vulnerabilities. Recent reporting by the National Cyber Security Center of the UK on APT29 activity confirms APT29 operating procedure includes exploiting recently detected software vulnerabilities (as described in Further TTPs associated with SVR cyber actors, and APT29 targets COVID-19 vaccine development).



As shown in Figure 1, communication within the infrastructure is cyclical. This indicates an automated framework that regularly communicates with, and possibly exfiltrates data from, the victim's email servers. This behavior includes what appears to be the actor, connecting to L2 OH over port TCP/8443 with anonymization through TOR at 8 PM UTC. This indicates that the actor likely included a Layer 3 host in the automated infrastructure setup. The observed infrastructure setup confirms APT29's ability to perform long-term automated operations. Such infrastructure provides APT29 with the ability to continuously acquire sensitive data from the targeted environment, highlighting the espionage focus of the group.

We recommend searching for and investigate any traffic from the listed layer 1 operator hosts.

This analysis isn't meant to be a complete exploration of the APT29 infrastructure but is representative of our ongoing analysis. The analysis performed in this report includes only a subset of the APT29 related IPs reported by RiskIQ, and the reader shouldn't necessarily assume these conclusions hold for the entire infrastructure.

How our visibility and actions help our clients

Our Threat Intelligence researchers monitor telemetry of suspicious traffic traversing our Global IP Network Service global Tier-1 IPv4/IPv6 backbone network for threat indicators. Correlating such findings with the insights of our global Threat Detection (TD) and Managed Detection and Response (MDR) services enables a truly unique perspective of the evolving cybersecurity threat landscape.

Research findings on threat actors and campaigns, such as APT29, are continuously being fed from our Threat Intelligence analysts back into our services as machine learning capabilities, behavior models, indicators of compromise and threat intelligence. This process enhances the service's ability to efficiently monitor, detect, triage and respond to these threats on behalf of our clients often without an initial compromise.

Indicators of compromise

Indicators of compromise where the L1 OH is sending traffic to the L2 OH on the same row:

Operator Host L1	Operator Host L2
190.97.165[.]202	141.255.164[.]40
45.114.130[.]81	111.90.151[.]120