The Anatomy of the DDoS Attack Campaign Targeting Organizations in Ukraine

netscout.com/blog/asert/ddos-attack-campaign-targeting-multiple-organizations-ukraine

by ASERT Team on February 17th, 2022

Overview

Beginning on 13 February 2022, multiple governmental, military, and financial organizations within Ukraine reported that their public-facing Web sites, applications, and ancillary supporting infrastructure were being targeted in an orchestrated DDoS attack campaign. Significant direct impact to these organizations and their direct constituents and customers, along with collateral impact to other organizations such as associated Web hosting operators, was noted.

Reports indicate that public access to online governmental services, online Web and mobile banking applications, and automated teller machines (ATMs) was disrupted by these attacks. The use of VPNs to connect ATMs across the public Internet to their affiliated networks is commonplace; when the associated financial network infrastructure is negatively impacted by DDoS attacks, bank patrons are often prevented from accessing funds, checking balance information, and performing other routine operations via ATMs.

NETSCOUT Arbor's ASERT team confirmed these reports, observing multiple direct-path (non-spoofed) SYN-flooding and UDP-flooding DDoS attacks targeting these organizations, along with a smaller number of NTP reflection/amplification DDoS attacks. Observed SYN-flood attack throughput reached a maximum of ~1.2 million packets-per-second (mpps), while large-packet UDP flooding attacks reached a maximum of ~5.3 Gbps. By way of comparison, the largest DDoS attacks reported in 2021 were ~674 Mpps and 3.47 Tbps, respectively.

The characteristics of all observed DDoS vectors utilized in these attacks to date were well within established norms and a trend we've observed over the course of 2021 for increases in botnet attacks; analysis of the attack dynamics indicates that standard DDoS-capable botnets were used in this attack campaign. Both DDoS-for-hire and privately-operated botnets are often used to generate DDoS attacks of the observed scale, scope, and types.

The brief spate of NTP reflection/amplification attacks observed at the beginning of the attack campaign, along with the direct-path UDP flooding observed throughout, are out of profile for the targeted networks/servers/services/applications, largely directed towards destination port UDP/443. The observed SYN-floods were primarily targeting destination ports TCP/80 and TCP/443, which is consistent with standard Web servers.

ASERT observed botnet nodes (bots) participating in these attacks located in Ukraine, Russia, Portugal, the United Kingdom, the United States, and New Zealand. Researchers at 360 Netlab reported that a Mirai botnet was used for the attacks with its command-and-control (C2) node located in the Netherlands. Analysis of the DDoS vectors utilized in this attack campaign are consistent with capabilities typically exhibited by Mirai botnets.

The number of observed sources utilized in this DDoS attack campaign to date are relatively low. This is consistent with the use of direct-path DDoS vectors and those utilized in these attacks, along with the reported attack volumes. Observed attack characteristics imply that any spoofing of source IPs which took place during these attacks was limited in scope, which comports with reports that the botnet in question was a typical Mirai botnet, with most of its constituent bots located on broadband access networks likely to enforce source-address validation (SAV; e.g., anti-spoofing).

Collateral Impact

Successful DDoS attacks against Web hosting and VPS operators can significantly impact organizations which are not the direct targets of DDoS attacks, but which share the same network/service/application/content-delivery infrastructure.

Disruption of online applications and services provided by governmental organizations can result in the inability to deliver critical services to their constituents.

Disruption of online financial services can result in delays in payroll deposits, bill payments, online and in-person electronic retail payments, ready access to cash, etc.

The collateral impact of reflection/amplification DDoS attacks is potentially quite high for organizations and individuals whose misconfigured servers/services are abused as reflectors/amplifiers. This may include partial or full interruption of mission-critical applications and services, as well as additional service disruption due to transit capacity consumption, state-table exhaustion of stateful firewalls and load-balancers, etc.

Individuals and organizations who's general-purpose and/or Internet-of-Things (IoT) devices have been subsumed into botnets can be negatively impacted when these compromised systems are utilized to launch outbound DDoS attacks. As with reflection/amplification attacks, this may include partial or full interruption of mission-critical applications and services, as well as additional service disruption due to transit capacity consumption, state-table exhaustion of stateful firewalls and load-balancers, etc.

Mitigating Factors

DDoS attack traffic can be mitigated via the implementation of industry-standard best current practices (BCPs) such as situationally appropriate network access control policies; network infrastructure-based reaction mechanisms such as flowspec; and intelligent DDoS mitigation systems (IDMSes) such as NETSCOUT Arbor Sightline, TMS, and AED.

Collateral impact to misconfigured, abusable computers/IoT devices/servers/services leveraged as bots or reflectors/amplifiers by attackers to launch DDoS attacks can motivate network operators and/or end-customers to remove or remediate affected systems.

Traceback of spoofed DDoS attack traffic to its ingress points by network operators and subsequent implementation of source-address validation (SAV) can prevent attackers from launching both reflection/amplification and spoofed direct-path DDoS attacks.

Recommended Actions

Organizations with business-critical public-facing internet properties should ensure that all relevant network infrastructure, architectural and operational Best Current Practices (BCPs) have been implemented, including situationally specific network access policies which only permit Internet traffic via required IP protocols and ports. Internet access network traffic to/from internal organizational personnel should be deconflated from internet traffic to/from public-facing internet properties and served via separate upstream internet transit links.

DDoS defenses for all public-facing Internet properties and supporting infrastructure should be implemented in a situationally appropriate manner, including periodic testing to ensure that any changes to organization's servers/services/applications are incorporated into its DDoS defense plan. Organic, on-site intelligent DDoS mitigation capabilities should be combined with cloud- or transit-based upstream DDoS mitigation services to ensure maximal responsiveness and flexibility during an attack.
It is imperative that organizations operating mission-critical public-facing internet properties and/or infrastructure ensure that all servers/services/application/datastores/infrastructure elements are protected against DDoS attack, and are included in periodic, realistic tests of the organization's DDoS mitigation plan. In many instances, we have encountered situations in which obvious elements such as public-facing Web servers were adequately protected, but authoritative DNS servers, application servers, and other critical service delivery elements were neglected, thus leaving them vulnerable to attack.

Specifics of countermeasure selection, tuning, and deployment will vary based upon the particulars of individual networks/resources; the relevant NETSCOUT Arbor account teams and/or ATAC may be consulted with regards to optimal countermeasure selection and employment.

flowspec can be used by network operators to mitigate UDP reflection/amplification DDoS attacks; direct-path UDP flooding DDoS attacks; and, in some circumstances, SYN-flood attacks, although intelligent DDoS mitigation systems (IDMSes) such as NETSCOUT Arbor TMS and AED provide a higher degree of mitigation granularity and interactive source evaluation when defending against SYN-floods. It is important to ensure that reaction access-control list (ACL) stanzas propagated via flowspec are configured in such a way to minimize the risk of overblocking.

AIF Templates providing examples DDoS countermeasure provisioning for standard server types are available to AIF-entitled Sightline/TMS operators. AIF Filter Lists of abusable reflectors/amplifiers are also available to AIF-entitled Sightline/TMS customers.

All potential DDoS attack mitigation measures described in this Summary *MUST* be tested and customized in a situationally appropriate manner prior to deployment on production networks.

Applicable NETSCOUT Arbor Solutions: NETSCOUT Arbor Sightline, TMS, and AED.

Additional References

https://edition.cnn.com/2022/02/16/europe/ukraine-cyber-attack-denial-service-intl/index.html
https://twitter.com/DougMadory/status/1493680334965297159

Posted In

Attacks and DDoS Attacks

Subscribe

Sign up now to receive the latest notifications and updates from NETSCOUT's ASERT.