



AAP

ADVANCED ADVERSARY PROTECTION

MONTHLY RISK SUMMARY REPORT

The following report supplies a brief summary of network and threat activity observed during the month of April. This information includes traffic analysis statistics as well as a summary of all event escalations.

If you have any questions regarding this report or its contents, please contact the Active Response Centre at arc@gosecure.ca.

Maintaining Your
Security Coverage

Traffic Analysis

Log Sources

Endpoint Detection
and Response

Alert and Observed
Threat Summary

Alerts Summary

GOSECURE
COUNTERTACK

ACTIVE RESPONSE CENTRE



Table of Contents

Maintaining Your Security Coverage.....	2
Personnel changes.....	2
Endpoint Protection.....	2
Infrastructure Updates.....	2
Traffic Analysis	3
Log Sources	4
Log sources no longer reporting.....	4
Endpoint Detection and Response	5
EDR Endpoint Count	5
Alert and Observed Threat Summary.....	6
Threat Priority.....	7
Alerts Summary	8

Maintaining Your Security Coverage

To help maintain the security of your environment, we ask that you consider the following items and ensure that AAP is fully integrated with your internal processes.

Personnel changes

When a member of your security team leaves your organization or transfers to another team, we ask that you inform the ARC so we can perform the following changes:

- Disable access to the AAP dashboard
- Issue a new Client ID to your organization
- Update your escalation path if required*

When a team member is added, please let us know if they require dashboard access, or if your escalation path will require updating.

*We highly recommend maintaining an email distribution list to help your team manage the list of personnel who receive communications from the ARC as these communications may contain sensitive information.

Endpoint Protection

To maintain endpoint protection, it is imperative that the latest Endpoint Detection and Response (EDR) agent be installed on all applicable assets in your environment. To accomplish this, we recommend the following best practices:

- Integrate the latest EDR agent into your golden images
- Include the latest EDR agent within your patching processes, keeping in mind the requirements for patch-related pending reboots to be completed prior to agent deployment
- Regularly cross reference your EDR deployment list (available from your client dashboard) with your asset management solution to ensure all endpoints are fully covered and reporting to our cluster, and that outdated entries in the EDR deployment list are removed

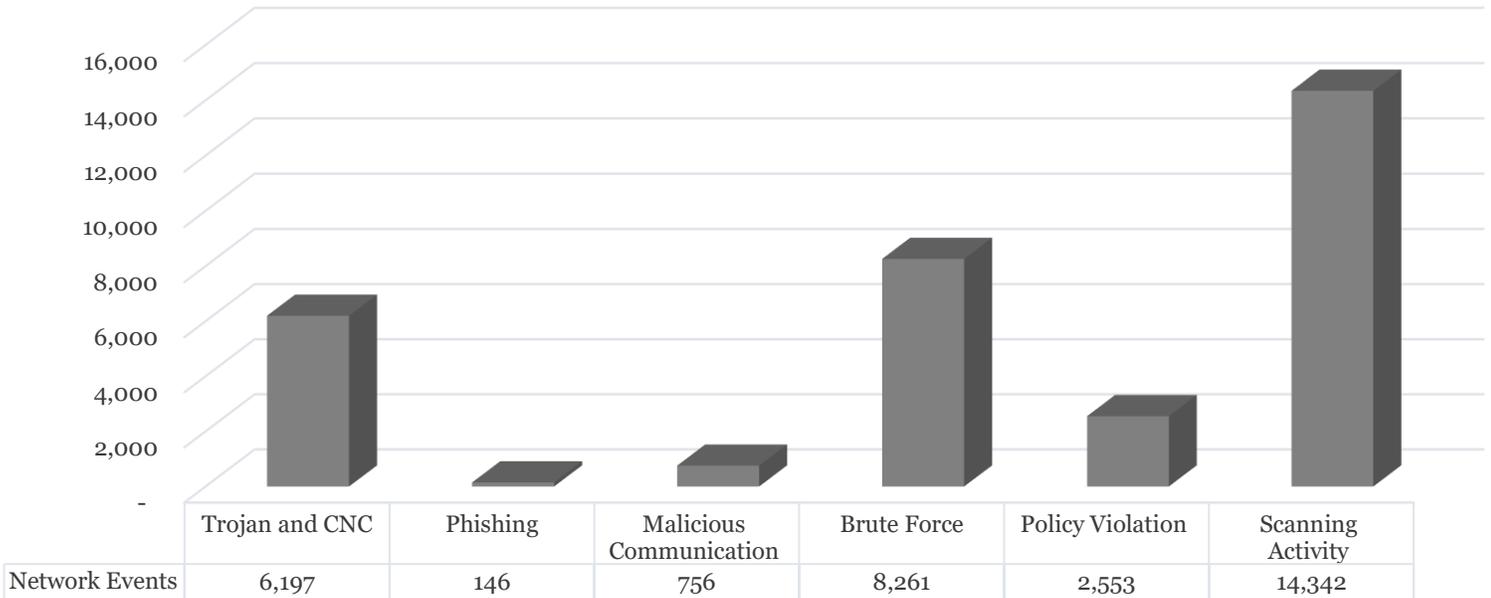
Infrastructure Updates

Following any alterations to critical infrastructure in your environment, we ask that you perform the following:

- Confirm your network spanning configuration to ensure the visibility of the ARC appliance has not been negatively affected
- Reference the logging sources page of the dashboard to ensure that the ARC is receiving logs from all required sources
- Provide updated network documentation to the ARC so we can update our situational awareness of your environment

Traffic Analysis

Below you will find a visual representation of the potentially malicious traffic observed during the month of April. After detection, all events are investigated to remove false positives and determine if the events pose a threat to your environment.



Traffic Type Categorization

Trojan/CNC Activity: Network traffic indicating potential compromised endpoints including communication to known command and control servers.

Phishing Activity: Email and website attempts leveraging social engineering techniques to manipulate users into clicking a malicious link or devolving personal information and credentials.

Malicious Communication: External Exploit Attempts, Malware, Spyware, Adware, Tool Bars or various other Potentially Unwanted Programs.

Brute Force Attempts: Attempts to gain access to internal systems by employing repeat password-guessing techniques.

Policy Violations: General policy violations including TOR traffic, P2P activity, explicit content and user credentials showing up in plain text or Base64 in outbound traffic.

Scanning Activity: External vulnerability scanners and attempts to gain private information about your network.

Log Sources

During the month of April we have received logs from **11 sources**. A comprehensive, live list of all log sources is available from your client dashboard.

Please note that clients are responsible for ensuring that all required logs sources are provided to the ARC for analysis. This list should be reviewed following any network changes to ensure that visibility has not been affected.

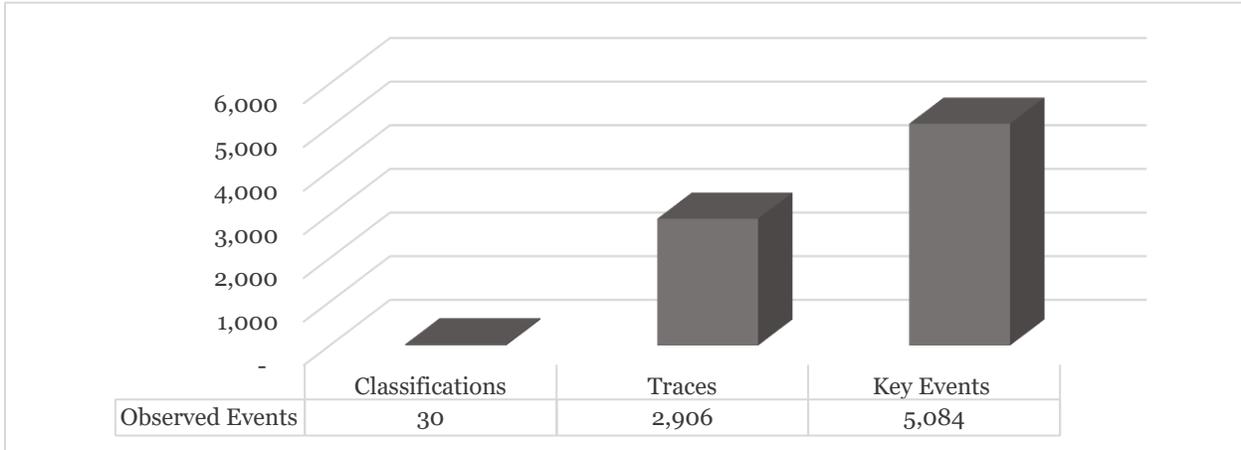
Log sources no longer reporting

The following sources have stopped providing logs to our appliance within the last 6 months. Please let us know which of these systems can be removed from the list as decommissioned log sources. Any unexpected list entries should be examined to ensure continued monitoring via the LIDS service.

Source	IP Address	Last Modified
FW-575	172.18.2.252	2019-03-30 15:14:32 UTC
FW-578	172.18.2.253	2019-03-30 15:03:13 UTC
FW-536	172.18.2.254	2019-03-30 15:03:03 UTC

Endpoint Detection and Response

There were over **322.7 million basic network events** analyzed for evidence of compromise during the month of April.



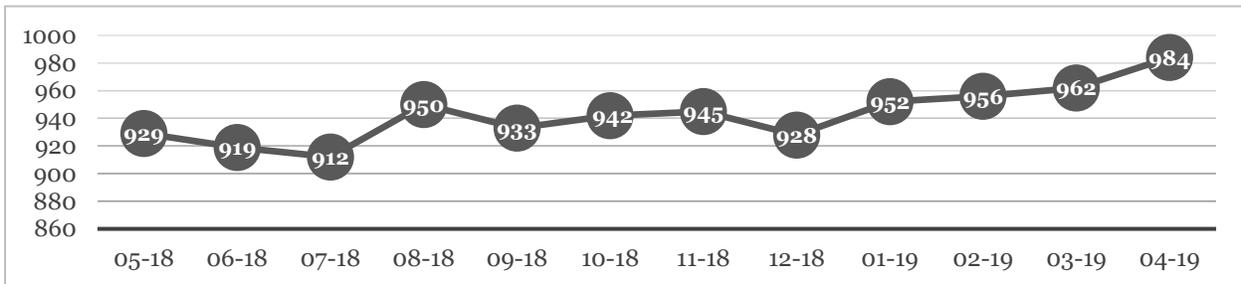
Classifications: Patterns of behavior characteristic of known malware families, techniques used by malware and other attempts to undermine endpoint integrity.

Traces: A set of related interactions starting from an origin event, following the evolution of activity over time. Used to provide context around suspicious interactions by exposing not only the suspicious interaction itself but the impact of that interaction on the operating system.

Key Events: Call out important interactions within a trace.

EDR Endpoint Count

At the time of this report there were **984 EDR agents** installed in your environment. A detailed account of all currently monitored endpoints can be obtained from your client dashboard. Agent deployment for your organization over time can be viewed in the below graph.

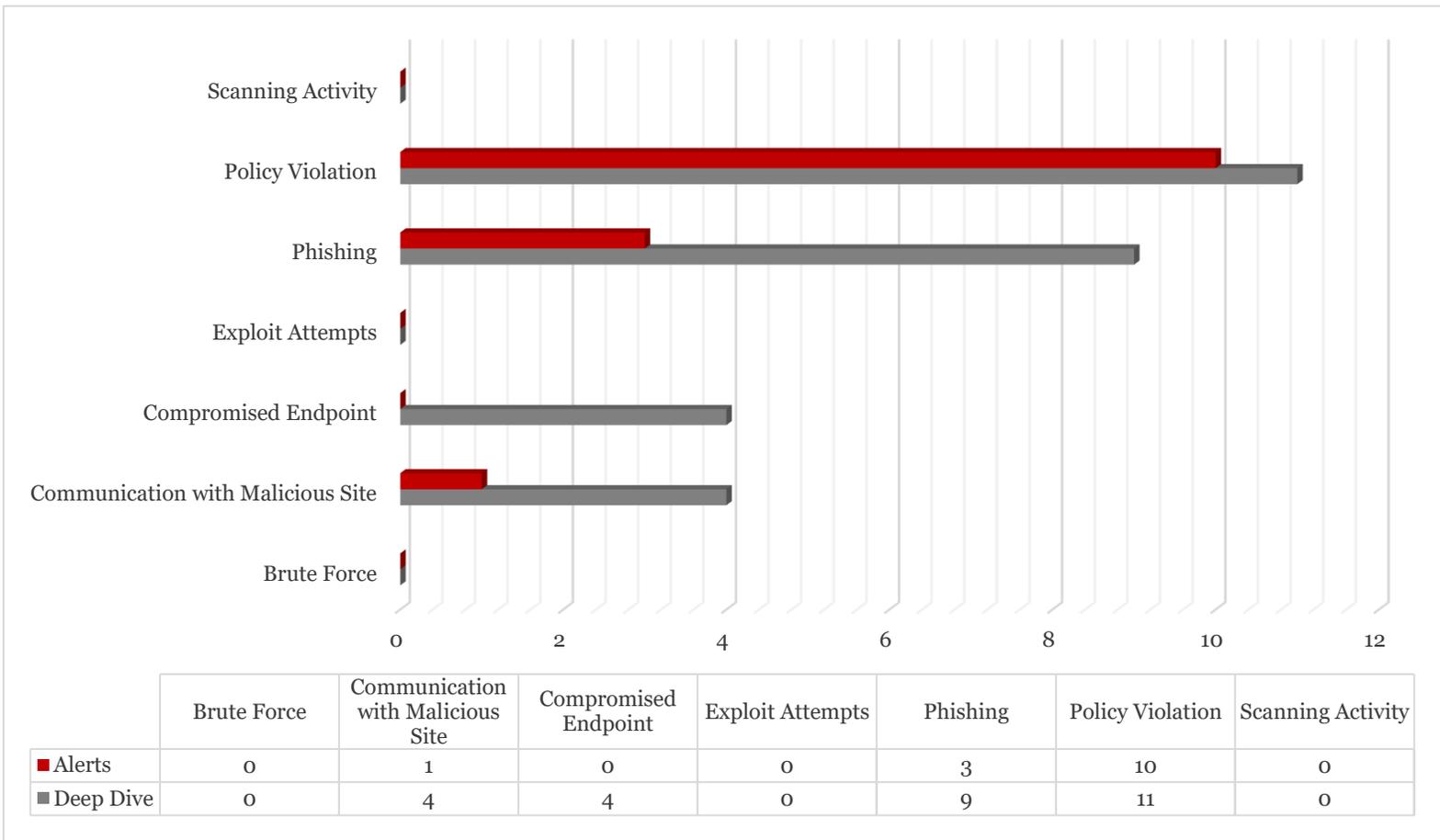


To ensure ongoing visibility, please ensure that the EDR agent is included in your golden images and patching process.

Alert and Observed Threat Summary

The threat activity summary demonstrates new potential threats observed interacting with your environment during the month of April.

The following graph serves to represent new threats only and does not show activity from sources previously investigated or alerted on. The numbers displayed are based on the volume of sources found, not the amount of activity seen from each of those sources.

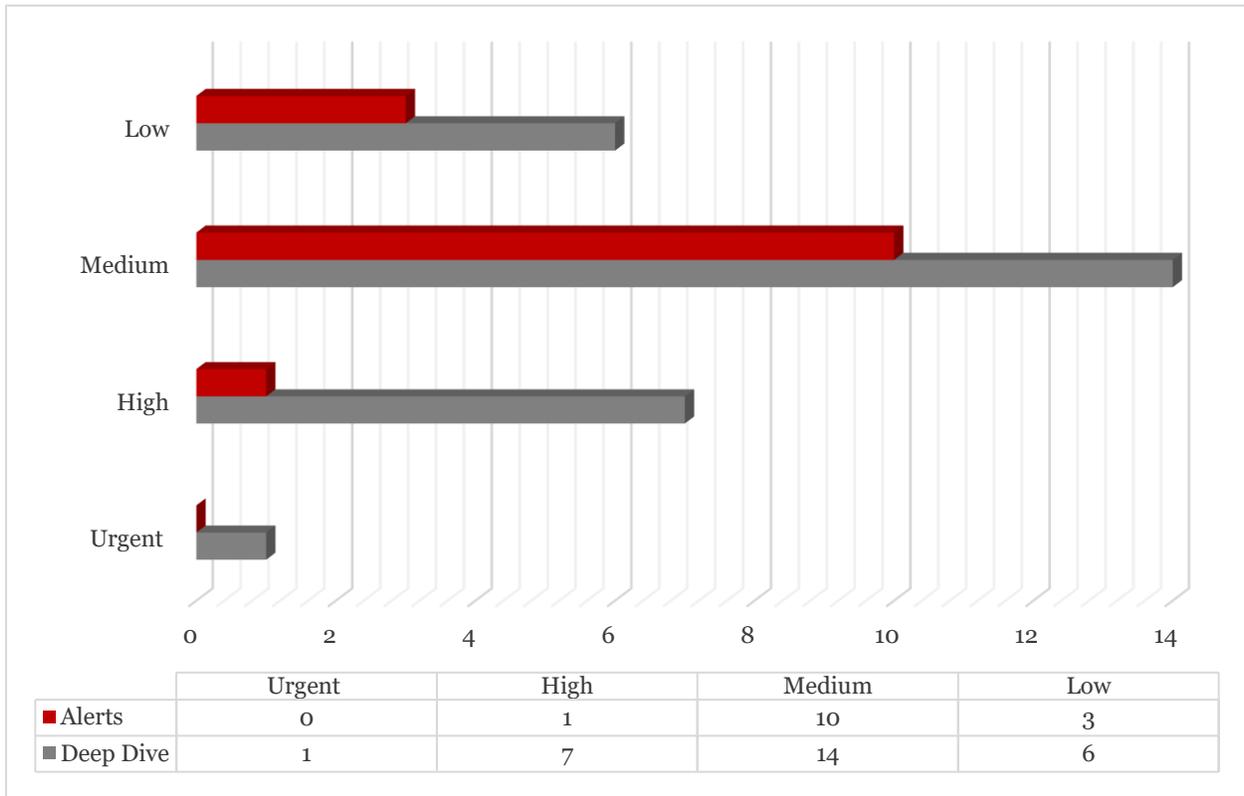


A “**Deep Dive**” is a security incident investigation that occurs when in-depth analysis is required to validate a potential threat and/or determine the impact of an incident that occurred. Only new threats spawn unique deep dives. If multiple events are related or the incidents follow the same pattern, they are collected in the same deep dive record to assist in ongoing pattern analysis.

The “**Alerts**” metric represents the alerts that have been escalated to your team divided by the type of activity observed.

Threat Priority

The following charts depict Alerts and Observed Threats for the month of April divided by priority level.



Urgent: High impact threats that cannot be mitigated by GoSecure. This includes successful phishing attacks and the compromise of endpoints where EDR is not installed. These events should be addressed by your security team as soon as possible.

High: High impact incidents such as the presence of a malicious file/email or compromised endpoints which have been placed in quarantine. Although these events should be dealt with as soon as possible, the threat is not spreading or actively exfiltrating data.

Medium: Potential threats including exploit and phishing attempts, recon scans and brute force activity. This activity should be addressed when resources are available.

Low: These events expose your organization to risk and increase the likelihood of a future compromise. Events in this category include: policy violations, potentially unwanted programs and user credentials visible in clear text. These events should be addressed to reduce risk to your organization.

Alerts Summary

Date	Ticket#	Status	Finding	Recommendation	Endpoint	Response
2019/05/02	201905020000192	Closed	We have observed malicious files Settlement_Copy_pdf.zip and Payment Confirmation Copy_pdf.zip on endpoint Tech1. These files were created on the endpoint as a result of opening an Outlook mail message.	Delete the files in question and perform a full set of bootable media anti-malware and anti-virus scans on the endpoint.	Tech1 10.10.10.04	These files have been removed. Thank you - Internal IT Security
2019/05/09	2019050910000013	Closed	We have observed communication between 10.10.10.5 and a known malicious or compromised domain, old[dot]yizhhd[dot]com, at IP address 195.154.53.99. The user was redirected to the malicious domain by visiting exoclick[dot]com, at IP address 64.111.199.222. *The endpoint with IP address 10.10.10.5 does not have the EDR agent installed.	Block the domain (old[dot]yizhhd[dot]com) and IP address (195.154.53.99) in question. Remove the endpoint from the network and perform a full set of bootable media anti-malware and anti-virus scans.	10.10.10.5	This ticket can be closed by following resolutions, 1, User machine was sent in and malicious software was removed 2, Destination was blocked on FW. - Internal IT Security
2019/05/15	2019051510000231	Closed	We have observed numerous indicators of compromise on endpoint Admin4 following the opening of malicious Word document March_Invoice#991029.doc, including the download of VBS file cYk4tb.vbs from file sharing service lithi[dot]io (104.29.16.19), and the attempted running thereof with wscript.exe. The endpoint was quarantined at 12:09 ADT. The event was discussed via phone call with your IT staff at 12:11 ADT	Remove the endpoint from the network and re-image. Change passwords for all accounts associated with the endpoint in question.	Admin 4 (10.10.10.9)	This endpoint has been reimaged and all associated passwords have been changed. Please close this ticket. - Internal IT Security
2019/05/16	2019051610000321	Closed	We have observed files associated with the Upatre Trojan downloader on endpoint Finance3. The files were created as a result of an Outlook email attachment. At this time we have not observed any indicators of compromise as the file has not been executed.	Delete the file in question and perform a full set of bootable media anti-malware and anti-virus scans on the endpoint.	Finance3 (10.10.10.19) User:Bob	Malicious files have been deleted and endpoint has been scanned. Please close this ticket. - Internal IT Security