Sample Agency

Malicious Domain Blocking and Reporting

06/05/2022 - 06/11/2022

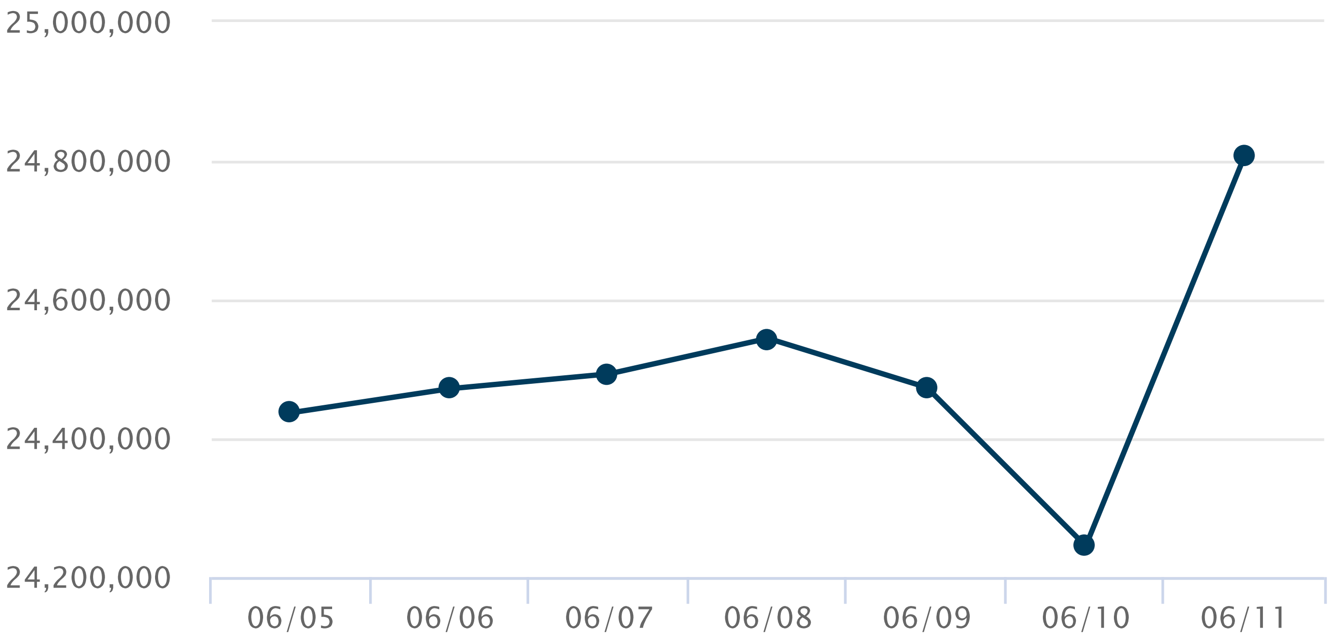
MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Elections
Infrastructure
ISAC®

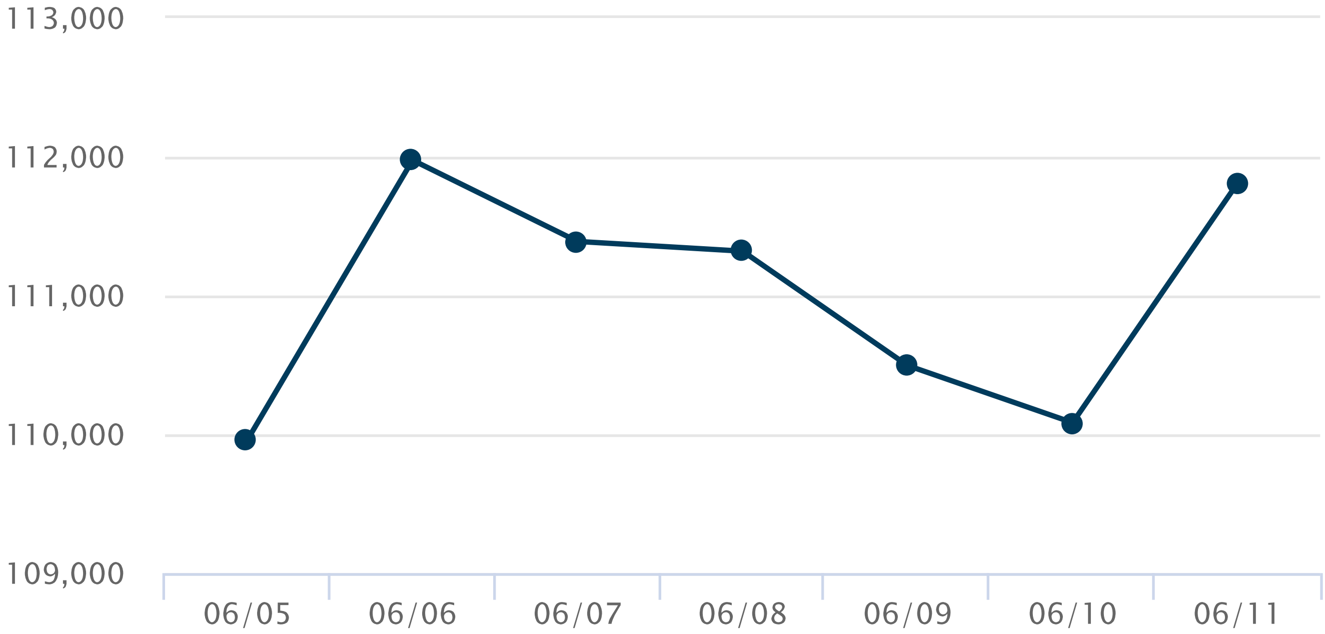
Confidential and Proprietary

During the week of 06/05, a total of 777,039 malicious DNS requests were blocked out of 171,471,097 requests, which accounts to less than 1% of all activity.

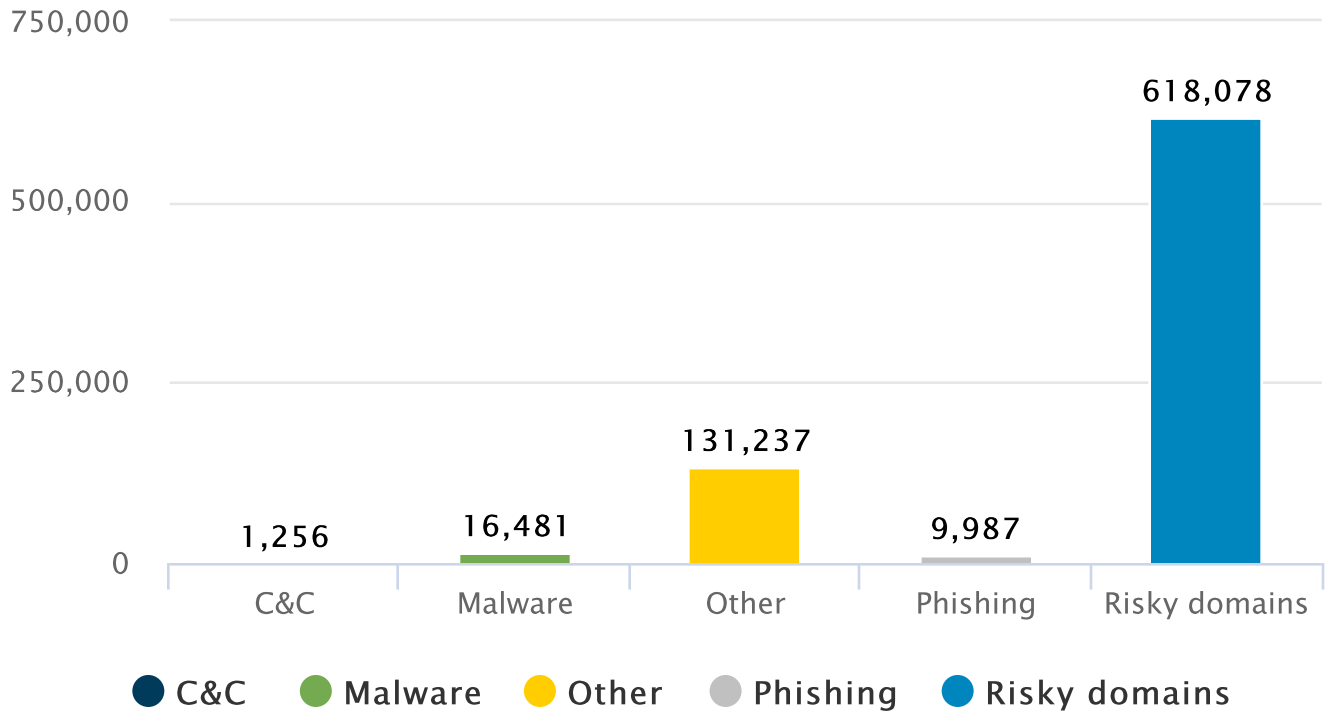
DNS Activity by Day



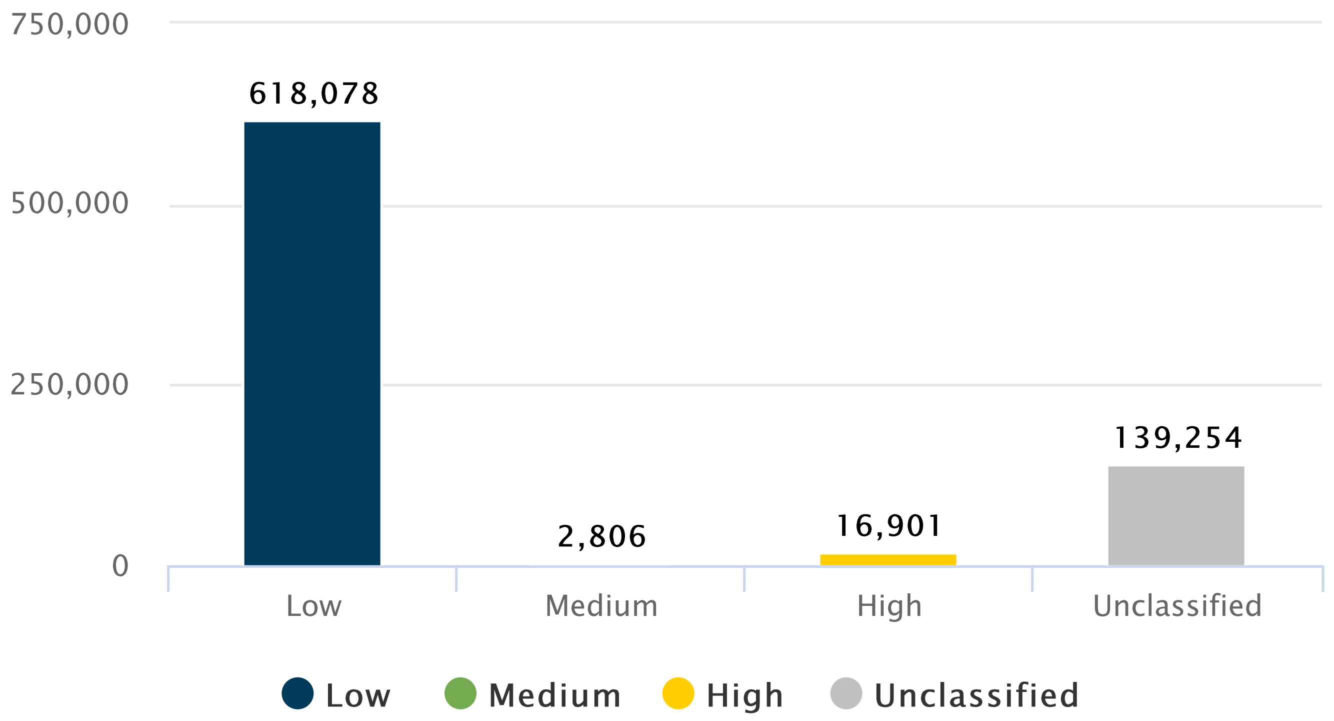
Blocked Malicious Domains by Day



Blocked Malicious Domains by Threat Category



Blocked Malicious Domains by Severity



Top 10 Blocked Malicious Domains

XXXXX[.]XXX

Number of Blocked Requests: 131,528

XXXXX[.]XXX

Number of Blocked Requests: 1,298
Description: This domain is used as malware
Threat: Known Malware [High]
Threat Category: Malware

XXXXX[.]XXX

Number of Blocked Requests: 1,274

XXXXX[.]XXX

Number of Blocked Requests: 768

XXXXX[.]XXX

Number of Blocked Requests: 677
Description: This domain is used as malware
Threat: Known Malware [High]
Threat Category: Malware

XXXXX[.]XXX

Number of Blocked Requests: 579
Description: This domain is used as malware
Threat: Known Malware [High]
Threat Category: Malware

XXXXX[.]XXX

Number of Blocked Requests: 428

XXXXX[.]XXX

Number of Blocked Requests: 416
Description: The domain is associated with multiple categories and therefore there is no enough information to decide to which category it's belongs
Threat: Suspected Malware [Medium]
Threat Category: Malware

XXXXX[.]XXX

Number of Blocked Requests: 379

XXXXX[.]XXX

Number of Blocked Requests: 365

[The top 10 domains listed above comprised nearly 18% of all blocked malicious domains for your organization.]

Appendix

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information and to ensure that sensitive information is shared with the appropriate audience. This is an international standard used by DHS, FBI, US-CERT, NCCIC, the U.K., Canada, Australia, New Zealand, and us to indicate who you can disseminate information to. If a recipient needs to share the information more widely than indicated by the original TLP designation, they must obtain explicit permission from the original source. Sources are responsible for ensuring that recipients of TLP information understand and can follow TLP sharing guidance. The latest TLP wording and coloring can be found at https://www.us-cert.gov/tlp

TLP: RED Not for disclosure, restricted to participants only. Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.

TLP: AMBER Limited disclosure, restricted to participants' organizations. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

TLP: GREEN Limited disclosure, restricted to the community. Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. TLP: GREEN information may not be released outside of the community.

TLP: WHITE Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.