MarkMonitor™

A Clarivate Analytics company

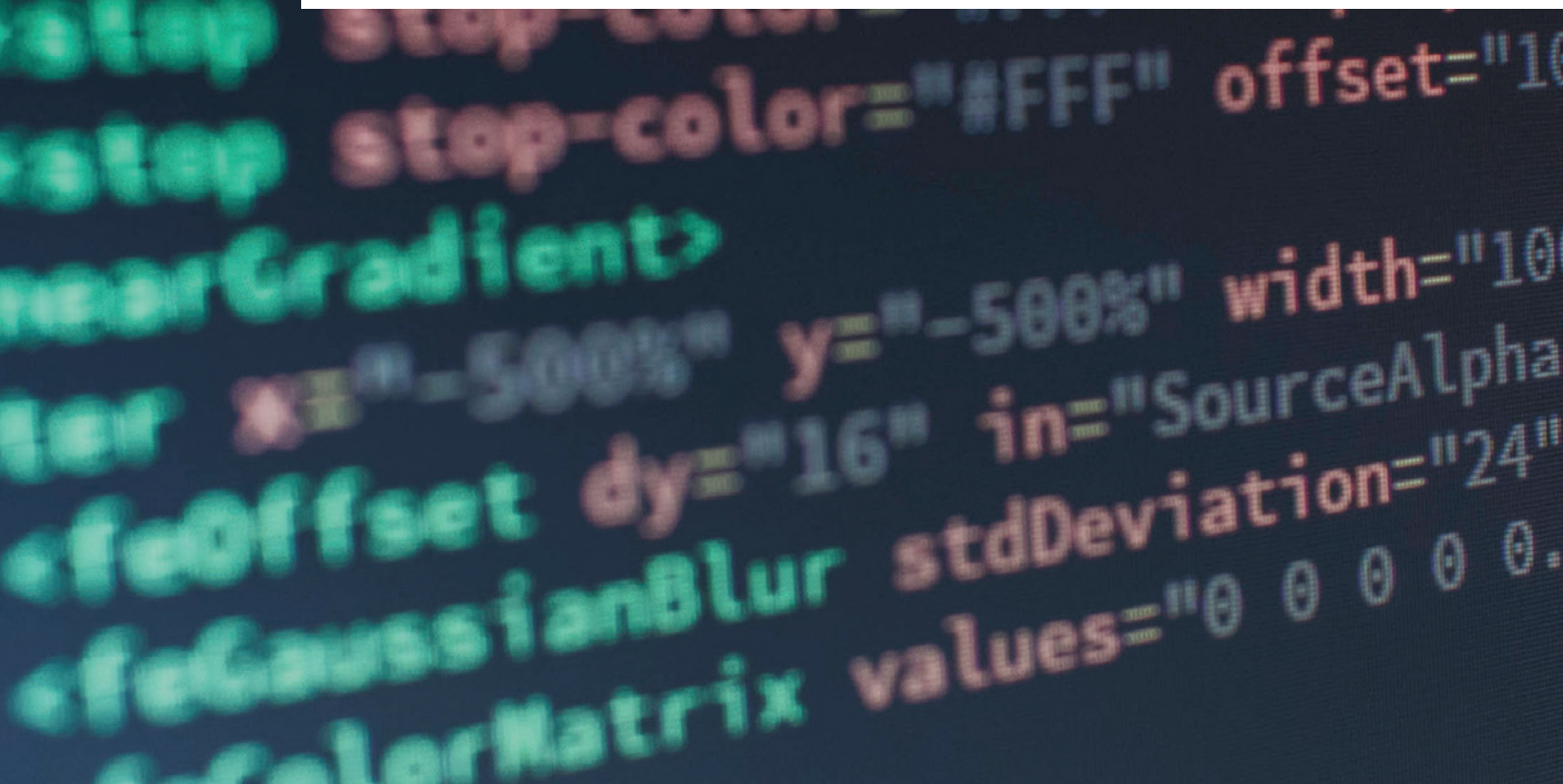
Fact sheet | Phishing Intelligence

Fight back against phishers targeting your brand

Data collected from phishing sites and kits can empower your organization to fight back against phishers targeting your brand.

MarkMonitor Phishing Intelligence is a feature of the MarkMonitor AntiPhishing Service designed to aid clients in protecting their organizations beyond whack-a-mole shutdowns. Collect data to help protect your customers – from victim credentials to lists of IP addresses that have accessed the phishing site – and shutdown email addresses that phishers use to collect credentials in order to combat phishers targeting your organization and customers.

Additionally, clustering phishing kits into related "families" can provide insight into volume of new phishing kits attacking your organization as well as other brands in your industry.



What is Phishing Intelligence?

- Data harvested from accessible files on a phishing site, this type of intelligence generally consists of harvested phish kits and phish log files.
- Discovered data from automated analysis of the phish kit can identify the online persona of the phisher who created or modified the phish kit, as well as the email collection point where victim credential information is often sent externally after it has been submitted to the phishing site. It is through this harvested data that phish kits can be clustered into related families.
- Phish log files harvested from the phishing site typically contain a cache of victim credential data or a list of IP addresses that have accessed the site.
- All phish kits and phish log files are harvested, analyzed, and clustered via automated processes and then stored in the MarkMonitor AntiFraud 24x7 online portal for quick and easy customer download.

How it works

When a phishing site is discovered, MarkMonitor collects site data via automated harvesters. The data collected includes the phish kit – which is the code powering the phishing site – plus any log files stored locally on the phishing site.

Phish log files can contain either victim credential files or a list of IP addresses that have accessed the site. If stored locally on the phishing site, victim credential files typically consist of the username, password, or other relevant personally identifiable information a victim submitted to the phishing site.

If the victim credential file is not stored locally, often the phish log file supplies a list of IP addresses and the date/time that IP addresses accessed the phishing site.

The phish kit data, meanwhile, yields relevant information about how the site was created and provides details on the phisher(s) who created or modified the phish kit. The collection point email address is a valuable piece of information that is used as a repository for credentials not stored locally on the phishing site. Email collection points can be shutdown to prevent the phisher from accessing their stored, stolen victim credentials.

Phish log files are harvested from the phishing site contain either:

- A list of IP addresses of possible victims who accessed the phishing site.
- A list of victim credentials submitted to the phishing site.

Harvested Phish Kits use unique identifiers to cluster kits into phish kit families:

- Collection point email addresses.
- Online usernames indicating the phisher who either created or modified the phishing kit.

MM384081785 / 01

Phish Kit Families:

- A MarkMonitor proprietary term, a "Phish Kit Family" is defined as multiple phish kits clustered together based on related identifiers. Identifiers can include kits either being created or modified by the same phisher, or having the same collection point email address used across multiple phish kits. They are determined to be related and are tracked as part of the same family.

- Related data that was harvested from the phish kit, like the phisher's online persona or the collection point email address, are then automatically clustered to track threat actors or multiple uses of the same collection point email addresses across all detected phishing sites and harvested phish kits.

- The value of tracking and clustering these data points is to allow you to see how heavily your organization and your industry is being targeted by new phishing kits and related phish kit families.

Using harvested data

With customer approval, when a collection point email address is harvested from a phish kit the MarkMonitor AntiFraud Security Operations Center can proactively shut down these email addresses, effectively preventing phishers from accessing that specific cache of stolen credentials.

If your organization tracks your customer IP addresses, then you can download and cross-reference the harvested phish log file of IP addresses that accessed the phishing site to determine if any of your customers accessed the phishing site.

Why is this valuable?

- This intelligence provides you the tools to be more proactive in protecting your customers, beyond whack-a-mole shutdowns – including identifying customer victims as quickly as possible.

- Phish kit family intelligence can be used when collaborating with law enforcement to pursue repetitious offenders.

- You may be able to implement protection steps within your threat intel/security environment with the intelligence provided.

Ongoing innovation for sustained support

MarkMonitor is committed to arming you with the data needed for escalations to law enforcement and for your communications around budget justification. Automated phish kit harvesting and clustering, and harvesting phish log files – all accessible as downloads from the MarkMonitor AntiFraud portal – provide ammunition to support proactive AntiPhishing efforts to protect your organization and customers.

Contact our experts today:

+1 800 745 9229 (U.S.)
+44 (0) 1978 528 370 (Europe)

markmonitor.com