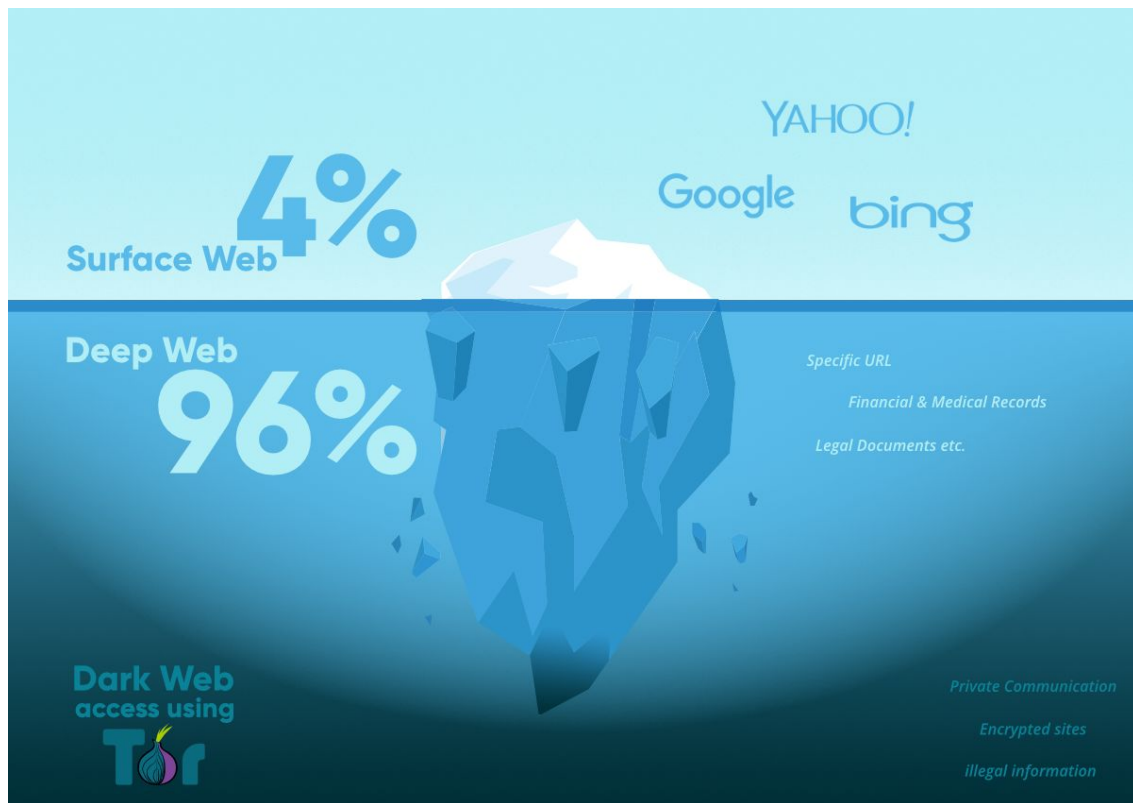




Threat Intelligence Services

The Surface, Deep, and Dark Webs



Most criminal activity requires a way to securely communicate or transact. The Internet provides a variety of avenues:

- Surface web forums supporting anonymity (e.g. 4Chan)
- Deep web forums requiring accounts
- Dark web marketplaces

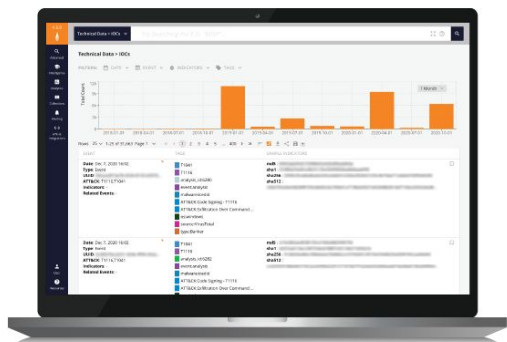
Deep and dark webs are not indexed by search engines!

Transactions are handled via cryptocurrency

Critical sources of intelligence for a variety of criminal activity

Often requires sensitive access and placement via relationship building

Flashpoint Solutions



FLASHPOINT INTELLIGENCE PLATFORM

Grants access to our archive of finished intelligence reports, data from illicit communities, chat services platforms, open web and technical data in a single, finished intelligence experience



Compromised Credentials Monitoring - Enterprise



Compromised Credentials Monitoring - Customer



Compromised Credentials Monitoring - Data Package



Data Exposure Alerting



Tailored Reporting Service



Threat Response and Readiness



Payment and Credit Card Fraud Mitigation



Domain Monitoring



Takedown Management



Managed Intelligence



Alerting

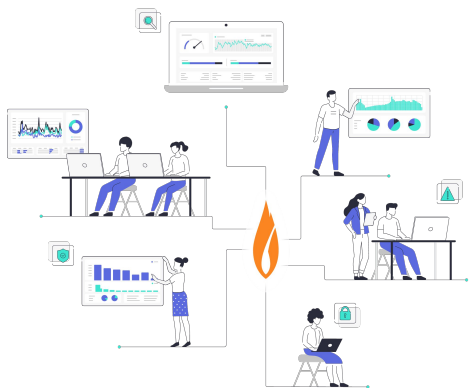


Extortion Monitoring Service



Request for Information (RFI)

Flashpoint Intelligence Impact Highlights from 2022



FLASHPOINT's combined human expertise, access to closed illicit communities, and proprietary data protected people, assets, and resources of our customers.

- A financial services customer detected more than \$4M in illicitly marketed assets, including checks and compromised accounts, using OCR capabilities
- A customer relied on Flashpoint's ransomware dashboard to regularly save them hours of time each week while supporting executive briefings
- During the month of June, a customer received 125 actionable alerts which equated to over \$15M in potentially averted losses
- An automated alert provided information to a customer that enabled their team to identify a threat actor's specific operations, saving them over \$5M.
- Flashpoint customers saved over 8K hours with Flashpoint Request for Information (RFI) custom analyst research intelligence.


Introducing the Threat Readiness and Response (TR2) Subscription



When an organization is targeted by ransomware or cyber extortion, it must quickly determine the extent of the attack, determine the response plan, and mitigate the impact. Flashpoint Professional Services offers a Threat Response & Readiness subscription that helps companies prepare for, as well as, quickly assess and respond to a ransomware or other cyber extortion attack.

Top Access Vectors

TIME TO COMPLETE	STAGE	PROCESS
Continuous Internet Scans	1	Gain Access
4 - 48 hours	2	Move Laterally
	3	Steal Data (Optional)
	4	Encrypt Systems (Speed)
2 days - 3 weeks	5	Ransom Note & Negotiation
Variable	6	Payment Decision
+6 months	7	Data Extortion & Ongoing Exposure



Top Access Vectors

- 1. Credentials / Phishing
- 2. Brute Force RDP
- 3. Unpatched Vulnerabilities

Are you vulnerable?

Username	Password
luis.sarmiento@ yoffices.com 🔍	[REDACTED]

Credentials Record Search

Your searches are logged and linked to your account, you should have a valid business reason to perform a search. See the [Usage Policy](#) for more info.

Search type: Custom Query (dropdown)
Enter query*: [REDACTED]yoffices.com
Exclude Combolists: No (dropdown)
Sort Field: Discovered At (dropdown)
Order: Desc (dropdown)
Search (button)

Results

Found 33 results in 4,697ms

Export Results (icon)

Username	Password	Domain	Affected Domain	Breach	Breached At	Discovered At	
mar mily	[REDACTED]	[REDACTED].c	-	Compromised Users from VirusTotal: Compressed File "530400be9b91e698367fc87a2e0106c8c071623d86be27ae4d6b89343a288bbb" Jun142022. 🔍	2022-06-14 T15:21:27Z	2022-06-14 T15:21:27Z	(i)
san yoff	[REDACTED]	[REDACTED].c	parkmobil e.io 🔍	Compromised Users from ParkMobile.io Apr082021. 🔍	2021-04-08 T12:00:00Z	2021-04-30 T16:02:50Z	(i)
edu offic	[REDACTED]	[REDACTED].c	-	Compromised Users From cit0day.in Breach Collection Combolist Nov012020. 🔍 premiumDatabases/ssgainstitutional.com [519.195] [HASH] (Business).rar	2020-11-01 T12:00:00Z	2020-11-03 T19:13:59Z	(i)

- OSINT searches confirm that Luis Carlos Sarmiento is the son of Colombia's wealthiest citizen, Luis Carlos Sarmiento Angulo
- Formerly employed at wealth management office

TR2: READINESS

- Combating Cyber Extortion Workshop: The workshop educates customer teams on the evolution of ransomware, attack vectors, profiles of attackers, cryptocurrency and issues related to payments, and other details relevant to the customer organization or vertical.
(Duration- 1 to 2 hours)
- Tabletop Exercises: The exercises will bring together critical stakeholders to discuss simulated scenarios, assess the efficacy of current plans, ensure clarification on roles and responsibilities, and improve coordination to help better mitigate future attacks.
(Duration 2-3 hours)



TR2: RESPONSE

- **Threat Actor Research:** Utilizing Flashpoint's experience navigating illicit online communities, Flashpoint will provide victim with available intelligence concerning the credibility of the threat actor's claims as well as their known tactics, techniques and procedures (TTPs).
- **Threat Actor Engagement:** Closely coordinated with victim, Flashpoint will manage and undertake all communications, interactions and negotiations with the threat actor.
- **Transaction:** Upon specific direction from and close coordination with victim, Flashpoint may deliver to the threat actor a ransom or other cyber extortion payment(s).
- **Delivery:** Securely provide to victim, any data, tool, or other information gathered as a result of the engagement with the threat actor.
- **Documentation:** Flashpoint will provide documentation of communications with the threat actor to include any payments made on the behalf of the victim.
- **Monitoring:** Flashpoint will conduct monitoring within Flashpoint's platform, containing expansive illicit online communities datasets, during and after the response.



OFAC Compliance Report Example

*Completed Prior to Any Payment

BUSINESS CONFIDENTIAL

FLASHPOINT

THREAT RESPONSE & READINESS SERVICE

OFAC Review Report -

As part of the Flashpoint Professional Services (PPS), the Ransomware Response offering helps teams in the event of a ransomware or cyber extortion incident. When other resolution efforts have not succeeded or are not feasible, Flashpoint may purchase the decryption keys and/or assurances from threat actors as part of its ransomware response services.

Flashpoint has years of experience in collecting threat intelligence from illicit actors responsible for many of the most prolific ransomware families. While Flashpoint will not necessarily have information on every threat actor, their history or their cryptocurrency transactions, we will work with Clients to help respond to a ransomware or cyber extortion attack – including whether and how to engage the threat actor, and whether and how to pay ransom or extortion demands.

OFAC Requirements

OFAC requires persons and entities making or facilitating payments to ransomware threat actors to exercise due diligence to avoid making payments that violate U.S. sanctions. Flashpoint has a due diligence process that it employs for those ransomware cases that require Flashpoint to purchase the decryption keys and/or assurances from the threat actor. In almost all cases, however, ransomware threat actors take significant steps to hide their identity. As a result, if Flashpoint cannot determine the threat actor's identity from its intelligence holdings, neither Flashpoint nor the client will know the identity of the individual with whom they are dealing or the country in which they are operating. Flashpoint strongly recommends notifying and consulting with law enforcement because law enforcement may have information to help identify the threat actor or country.

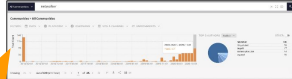
CONFIDENTIAL

Flashpoint Intelligence

BUSINESS CONFIDENTIAL

Flashpoint Due Diligence Review in Support of

- The following selectors were obtained from the **Hexxer** ransom attack against:
 - Threat group name: **hexxer**.
 - Domain Sites: [REDACTED]
 - Bitcoin address: [REDACTED]
- Flashpoint will conduct a search within the Flashpoint platform (FP2005) for information about the specific ransomware threat actor and/or the wallet to see if there is any owner identity or geographic location information on **FP2005**, to use to search OFAC's Consolidated Sanctions List data files, as well as any indication that the threat actor has successfully targeted others, and if so, whether they have produced information in return for ransom payments.



Flashpoint maintains collection on **hexxer**-related actors dating back to 2016. It also has active collections on the onion sites used to post stolen data from impacted victims to receive ransom payments. "**hexxer**" ransomware also known as "**hexx0r**" was originally discovered in August 2019. On March 20, 2020, threat actor "**hexx0r**" posted on the top tier Russian-language cybercrime forum XSS offering **hexx0r** as a ransomware-as-a-service (RaaS).

- The **hexx0r** group publishes data online if victims do not pay the ransom fee. The group's blog is located at above onion sites and can be found in **FP2005**. At this time, there are no indications [REDACTED] data is exposed on any of the sites they maintain.
- There is no information in **FP2005** as it pertains to the bitcoin wallet.

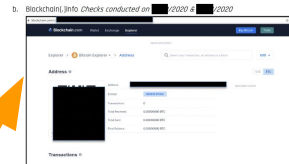


CONFIDENTIAL

Blockchain Analysis

BUSINESS CONFIDENTIAL

- Flashpoint will review the history of the wallet using open source and/or third-party cryptocurrency tracking tools into which the ransom is being demanded.
 - Flashpoint conducted open source and bitcoin tracing technologies. The identified bitcoin wallet has no history of transactions.



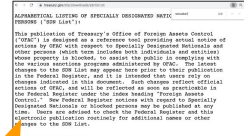
- Flashpoint will coordinate with Law Enforcement. Flashpoint will promptly, responsibly, and in good faith confer with client to determine whether, to what extent, when, and where should engage with any law enforcement or governmental authority with respect to a specific incident.
 - [REDACTED] is coordinating with their local FBI field office.
 - Flashpoint's owners the Baltimore FBI field office is the primary office leading investigations into the **hexx0r** ransomware group. At this time, there is no data from the FBI field office that **hexx0r** group is listed on the OFAC SDN list.
 - FOI: [REDACTED]
- Complete the Flashpoint "Ransomware Response OFAC Review Process" form to document pertinent searches against OFAC list.
 - hexx0r** Search on OFAC yields no results. <https://www.treasury.gov/ofac/downloads/sdnlist.txt>

CONFIDENTIAL

Contemporaneous Record Keeping of Sanctions Lists

BUSINESS CONFIDENTIAL

Checks conducted on [REDACTED] [REDACTED] [REDACTED]



coin wallet search yields no results <https://www.treasury.gov/ofac/downloads/sdnlist.txt>

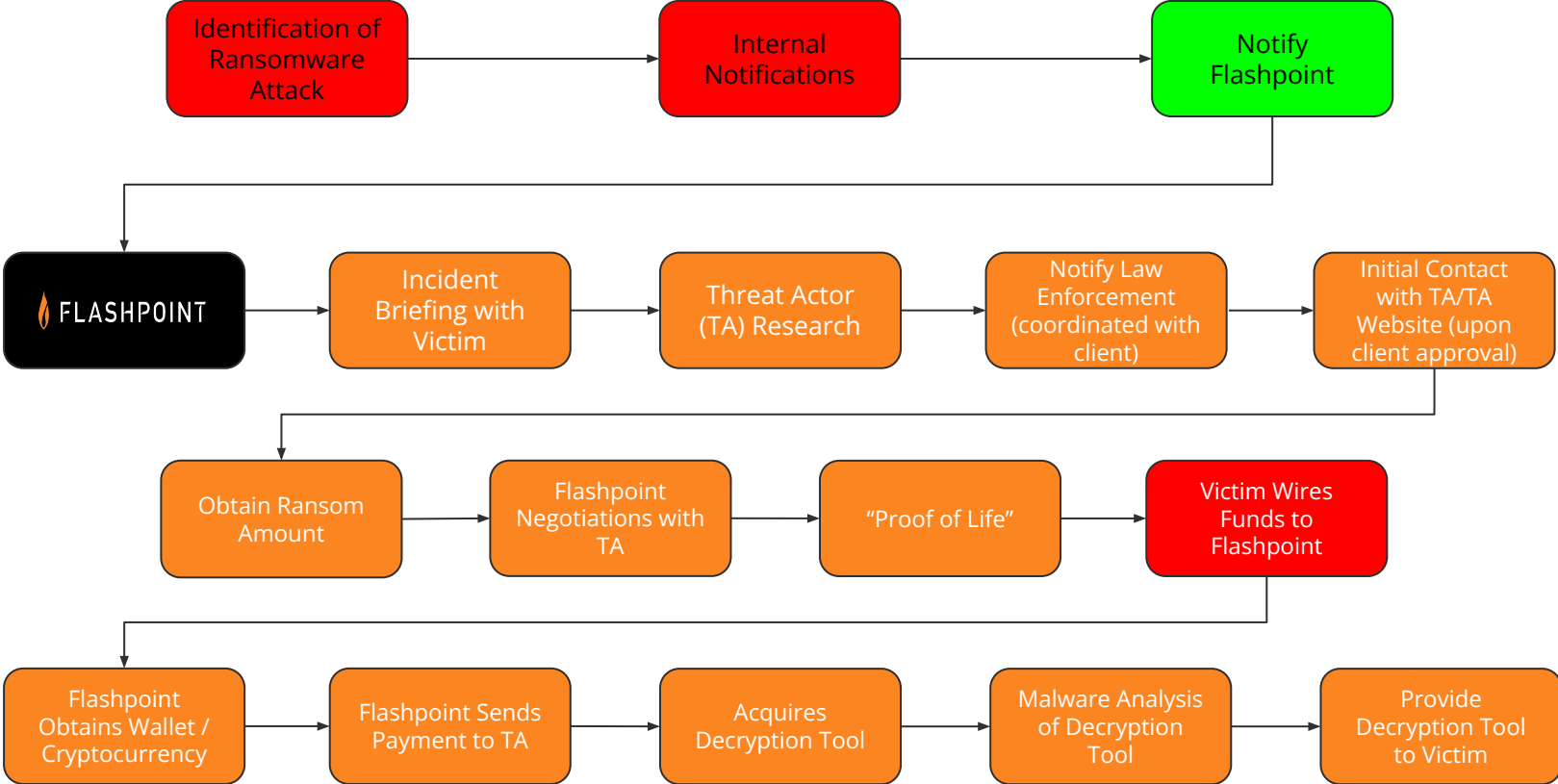


EU Consolidated Financial Sanctions List yielded no results for **hexx0r**. <https://www.europa.eu/eu/rapid/en/content/consolidated-list-of-persons-and-entities-subject-to-eu-financial-sanctions-response-202006-2446-418-8206-0000004119>



CONFIDENTIAL

Extortion Workflow Process



TR2: Key Benefits

- Develop contingencies in the event of an attack, including establishing a process to ensure payments can be made securely and quickly.
- Prepare in advance of an incident with training and education, and assist in rapidly acquiring cryptocurrency in the event of an immediate attack.
- Access to Flashpoint subject-matter experts (SMEs), providing the necessary intelligence to support a number of critical assessments, starting with the determination of whether an attack is a legitimate ransomware or extortion situation.
- Monitoring within Flashpoint's expansive datasets for any discussions about the attack and leak of victim's data.

 FLASHPOINT

Questions?



Thank You!

advisor@flashpoint.io