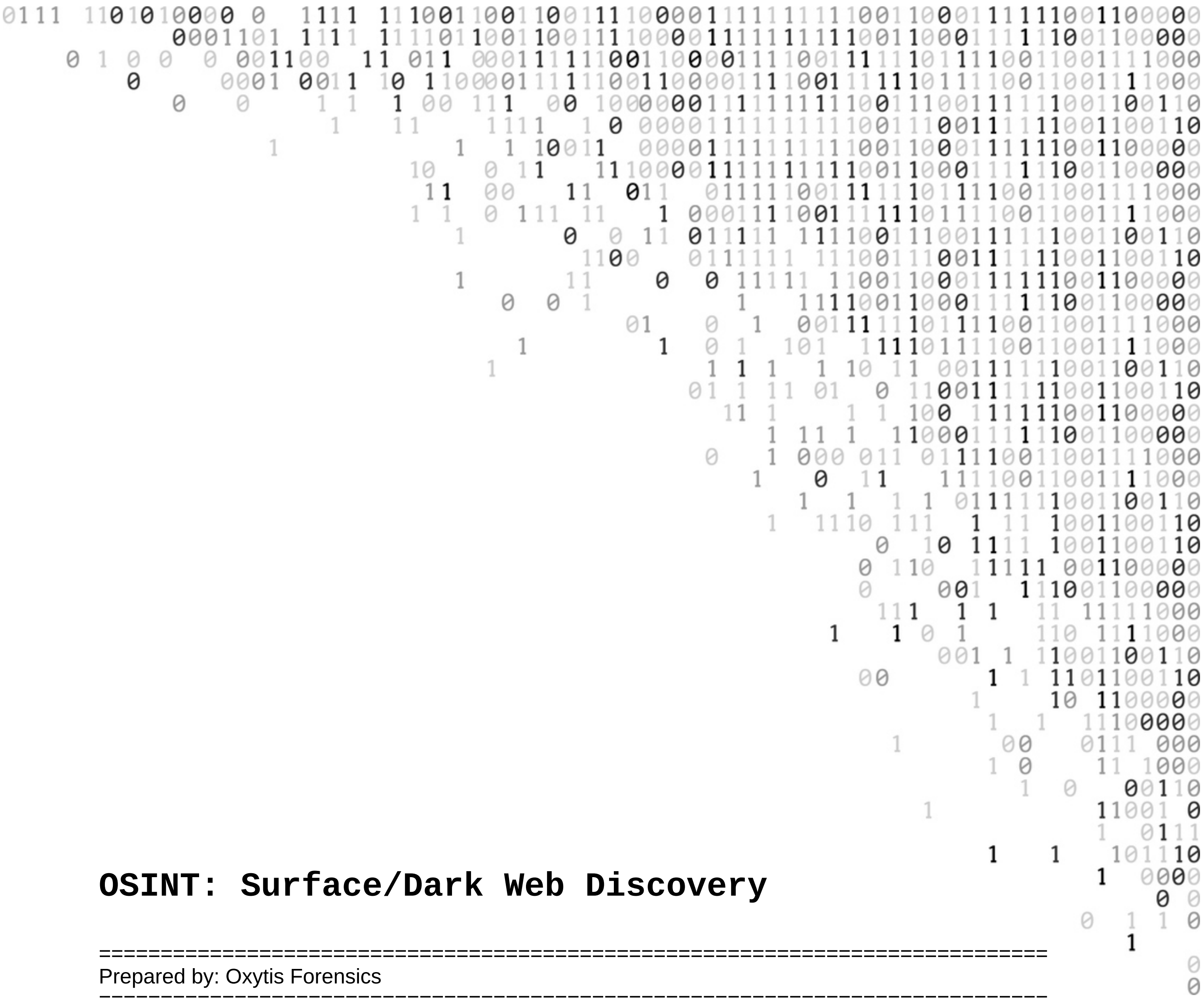

OSINT: Surface/Dark Web Discovery

==

Prepared by: Oxytis Forensics

==

cynergistek.com

==

Date: 18 January 2023

==

OSINT: Surface/Dark Web Discovery

External Discovery

Oxytis Forensics OSINT methods attempt to discover leaked credentials and other incidental data. During OSINT we search for use of credentials in other third party services that could have minimal security protection and consequently offer an opportunity for attackers. We also look for indication of phishing services that are set up to appear to belong to cynergistek.com. Oxytis Forensics attempts to find incidental or leaked documents that reside in places like pastebin, forums, search engines, and various social media sites. For example, monitoring Internet sites known to traffic information about organizational data on the dark web and open Internet could reveal active campaigns in progress.

Subdomains Registered: 59

['sft', 'mail', 'tektrak', 'zixvpm', 'trout', 'autodiscover', 'ssh', 'sites', 'teamspeak', 'blog', 'qa', 'dev', 'docs', 'www', 'execasst', 'tw-25434', 'cayenne', 'localhost', 'phishing', 'qr', 'mailchimp', 'pat', 'insights', 'em', 'quality', 'enterpriseenrollment', 'lyncdiscover', 'leads', 'files', 'registration', 'angler', 'support', 'frank', 'betty', 'components', 'dave', 'cloudflare-resolve-to', 'go2', 'video', 'selector1._domainkey', 'podcast', 'sfdc2._domainkey', 'hammerhead', 'sip', 'staging', 'reporting', 'crm', 'calendar', 'opsdb', 'aji', 'rpa', 'ftp', 'barracuda', 'mango', 'selector2._domainkey', 'vpn', '_dmarc', 'marlin', 'ts']
...

Domains (Typosquatting): 8

Typosquatting attacks start with cybercriminals buying and registering a domain name that is either a misspelling, alternative spelling, hyphenated, or wrong domain ending .

['cynergistek.ws', 'cynergistek.org', 'cynergistek.net', 'cynergistek.co', 'cynergistek.com', 'xn--cynergistk-j7a.com', 'cynergistek.health', 'xn--ynergistek-n6a.com']

Harvested Emails: 12

Hackers find it useful to perform online password attacks and it is important to know the IDs or usernames before commencing the cracking process during targeted attacks. The list of email addresses can also be used for the purpose of mass mailing, phishing, or spear phishing.

['marti.arvin@cynergistek.com', 'bryan.flynn@cynergistek.com', 'jana.langhorne@cynergistek.com', 'investorrelations@cynergistek.com', 'info@cynergistek.com', 'lauren.frickle@cynergistek.com', 'trinity.mcpherson@cynergistek.com', 'benjamin.denkers@cynergistek.com', 'advisory@cynergistek.com', 'board@cynergistek.com', 'investorrealtions@cynergistek.com', 'coryn.blacketer@cynergistek.com']

Stolen Credentials (Dark Web): 0

Querys a database of millions of computers which are compromised through global info-stealer campaigns performed by threat actors. The database is updated with new compromised computers every day through purchases of compromised data directly from top-tier threat actors operating in closed circle hacking groups.

Leaked Credentials: 6

A breach in this context is defined as an incident where data has been unintentionally exposed to the public. The Oxytis Forensics surface web monitoring and reputation management services are designed to monitor, detect and potentially suppress or remove unwanted information found on the web.

marti.arvin@cynergistek.com
- Adapt
- Apollo
- PDL

bryan.flynn@cynergistek.com
- Apollo

jana.langhorne@cynergistek.com
- Adapt

Apollo
db8151dd
DataAndLeads
PDL
Exactis
LinkedInScrape
MGM2022Update
NetProspex
VerificationsIO
YouveBeenScraped

trinity.mcpherson@cynergistek.com
advisory@cynergistek.com
investorrealtions@cynergistek.com