EVERYTHING TO KNOW ABOUT RANSOMWARE

From the Anatomy of Ransomware Attacks to the OSINT Tools for Ransomware Investigations

MALTEGO

whitepaper

Table of Content

Executive summary

Ransomware is a type of software that encrypts users' data, ensuring that they can no longer recover it without payment. It has been around since about 1989 and has become a very lucrative business with a bleeding impact on organizations: Financial cost of pay-out, loss of reputation, agencies' fines, permanent data loss, operational loss, clean-up/damage repair costs. As ransomware attacks rise alongside the massive adoption of technology and cryptocurrency, they have also evolved to implement non-monetary extortion threats and RaaS (Ransomware-as-a-Service) strategy to urge victims into submitting payments.

In this whitepaper, we will guide you through the anatomy of ransomware attacks—including the threat actors, their operational processes and roles, and more—as well as the investigative workflows, data, and tools that support effective ransomware investigations.

Key Takeaways

- Around since 1989, ransomware is a type of malware that encrypts the victim's data and only giving them access once payment, or a ransom, has been provided.
- IBM Ponemon Institute states that the average cost of a ransomware breach in 2021 was estimated at $4.62 million. Chainanalysis states in their 2021 report that ransomware payment size was over $118,000 in 2021, up from $88,000 in 2020 and $25,000 in 2019, with some large payments such as the record $40 million received by Phoenix Cryptolocker.
- Threat actors nowadays follow a collaborative operational model called "Ransomware-as-a-Service (RaaS)" and divide the operation into three roles: Operators, Affiliates, and Initial Combat Brokers.
- Ransomware investigations usually involve the following steps: Mapping the threat landscape, identifying attach surface, threat hunting in internal networks, TTP investigations, and finally, follow-the-money investigations.
- Maltego provides a number of data integrations to aid the different steps in a ransomware investigation and helps investigators easily visualize data relationships between data points from different data sources.

Understanding Ransomware Threats

Although it has been the most remarkable cyberthreat in the last years, ransomware is not something new in the cybersecurity arena: The first malware asking for a ransom payment dates back to 1989. The invention of Bitcoin in 2008 (facilitating anonymous payments), the professionalization of cybercrime growing up heavily a few years later (strong collaboration and exchange in dark web hacking forums and markets), and the massive adoption of technology (with relevant vulnerabilities and high-impact exploits from time to time) has probably generated the "perfect storm" for them.

					RANSOMWARE GOES BIG				
	1989 AIDS Trojan	2005 - 2006 GPCode Archiveus	2008 Bitcoin	2012 Reveton	2013-2015 CryptoLocker	2016 Ransom32 Locky	2017 Wanna Cry Petya	2018 New Variants	2019 MegaCortex
Threat	Local Symmetric Encryption	Assymetric Encryption	Invention of Bitcoin	Threats of Criminal Prosecution	Online Assymetric Encryption			Detection avoidance Backups deleted Forensic evidence destroyed	
Delivery	Physically Mailed Floppy Disks	Trojans		Trojans	Online Trojan Email attachments	Online Trojans Email Phishing	Exploit-based propagation	Exploit-based propagation Phishing	Exploit-based propagation
Payment	Payoff to Banks	Website Purchases		Prepaid cash services	Bitcoin	Bitcoin	Bitcoin	Cryptocurrency	Cryptocurrency

Ransomware Evolution: Timeline from 1989 to 2019

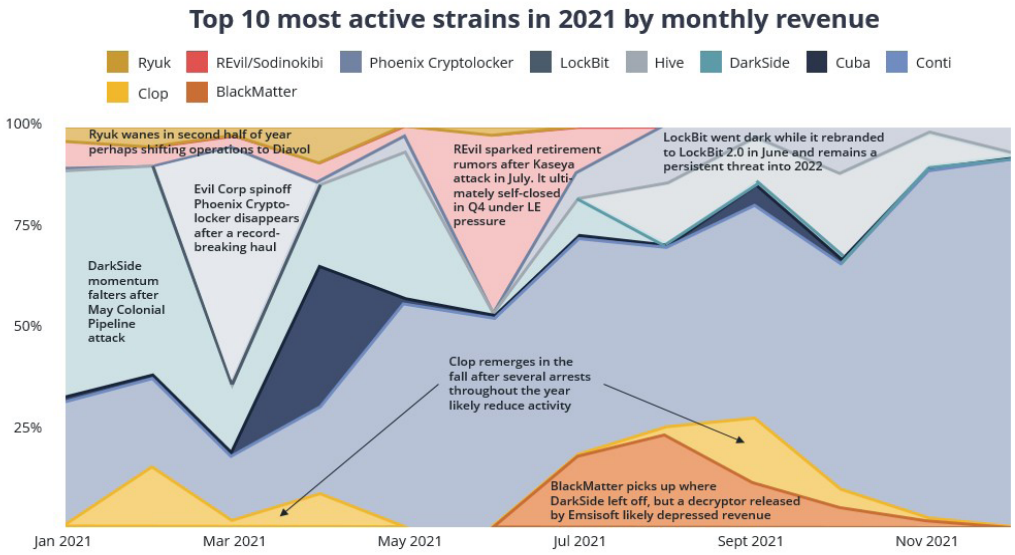
IMAGE SOURCE: TECHSPOT.COM

Ransomware, as a malware specimen, is a relatively simple piece of software that encrypts a victim's data, making it theoretically unrecoverable, and demanding payment in exchange for recovery. It is mainly used by threat actors during the last stage of a network compromise. This means that, before its detonation, an initial entry vector was abused, and several steps were taken afterward to silently pivot and land into other highly relevant assets in the organization. During that breach, attackers will be trying to obtain enough privileges to launch data encryption and wipe everything out, including mirrored data and online backups, even hosted in alternative systems for business continuity purposes.

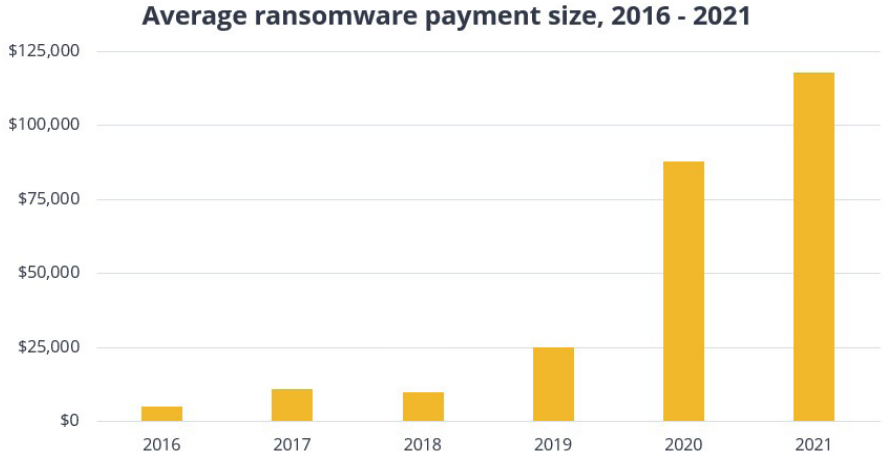
It must be noted that their extortion activities do not just stop at asking a ransom for data recovery, but also heavily pressuring victims by threatening to leak stolen information, including customer data, intellectual property, etc.

IBM Ponemon Institute states that the average cost of a ransomware breach in 2021 was estimated at $4.62 million[1]. We are talking about a very lucrative business with a bleeding impact on organizations: financial cost of pay-out, loss of reputation, agencies' fines, permanent data loss, operational loss, clean-up/damage repair costs.

Chainanalysis states in their 2021 report that there were more active ransomware strains than any other year, at least 140 of them received payments from victims at any point in 2021, compared to 119 in 2020, and 79 in 2019. The same study indicates that ransomware payment size was over $118,000 in 2021, up from $88,000 in 2020 and $25,000 in 2019, with some large payments such as the record $40 million received by Phoenix Cryptolocker. One reason for the mentioned increase in ransom sizes is ransomware attackers' focus on carrying out highly targeted attacks against large organizations.



REFERENCE: CHAINANALYSIS



REFERENCE: CHAINANALYSIS

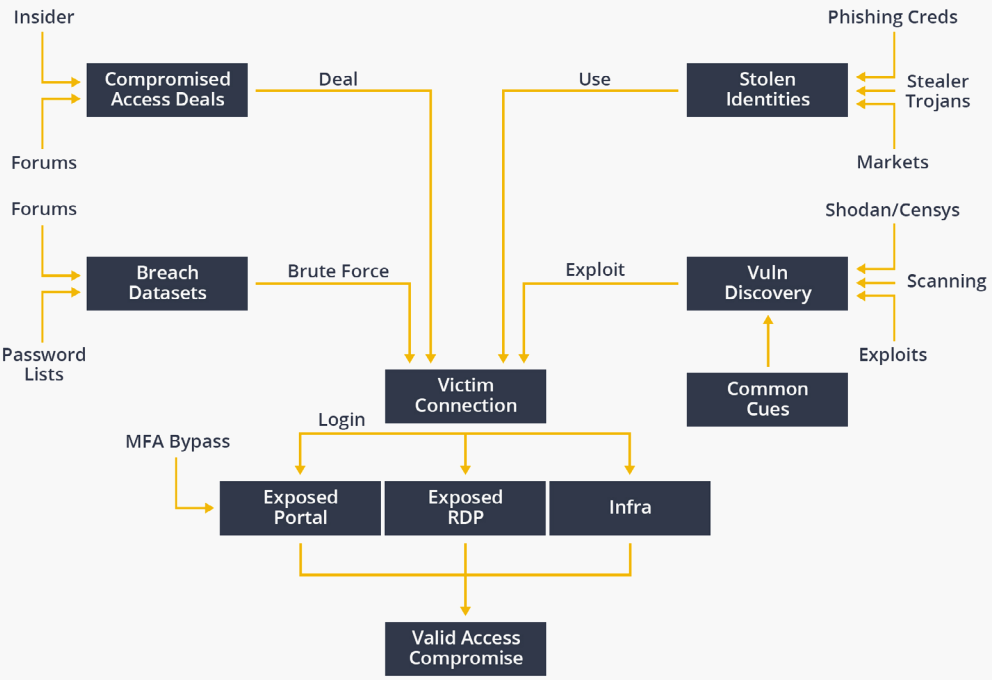
1. IBM PONEMON "COST OF A DATA BREACH REPORT 2021"

Ransomware Players

As you will notice, there are many stages and different tools involved in a ransomware attack. The criminal hacking industry, as in any other software and services one, requires specialization and a strong partnership program as the most reasonable step to compete in this business. Nowadays, this is no longer a "*Blue Ocean*" as there are many threat actors competing to compromise a big ecosystem.

The most common trend in this ecosystem is following a collaborative operational model known as Ransomware as a Service (RaaS) with three clear roles:

Operators	• Core of the criminal business • Building and maintaining the ransomware • Capturing the best affiliates/partners for intrusions • Brand/service advertisement to compete with rival operators
Affiliates	• Individuals or small teams partnering with Operators • Compromising victims' networks in order to deploy ransomware • Heavily exploiting vulnerabilities in exposed systems • Owning or using a malware distribution service
Initial Access Brokers (IABs)	• Individuals or small teams without an unclear partnership with affiliates • Use scanning tools to identify vulnerabilities and exploit those flaws • Selling access to the highest bidder for a one-time price or negotiating a fee • Mostly using long-standing vulnerabilities in common software and systems



REFERENCE: CURATED INTEL IAB LANDSCAPE

Considering several reports published by relevant Cybersecurity organizations, including US CISA, NCSC-UK and Australian Cyber Security Centre (ACSC) there are some common trends to consider in Ransomware groups:

- They are **sharing victim information** with each other, diversifying the threat to targeted organizations.
- They are **diversifying approaches to extort money** from "double" to "triple extortion" by threatening to (1) publicly release stolen sensitive information, (2) disrupt the victim's internet access, and/or (3) inform the victim's partners, shareholders, or suppliers about the incident.
- They are **growing up their business model** increasing activities using RaaS strategy with additional services such as payments negotiation, assisting victims with the payment or restoration process (24/7 help center), arbitration of disputes between themselves and other cybercriminal groups.
- They are **using different criminal infrastructure** to carry out attacks, such as bulletproof web hosting, domain registration services, botnets, proxy services, email services, etc.
- They are extensively **using hacking tools** to scan and identify vulnerabilities in victims' networks and efficiently distributing ransomware once the domain has been compromised.
- They **have a clear timing strategy** to target during holidays and weekends as they are attractive timeframes for a major impact without being noticed by some early warnings.

At the same time there are some common trends to be considered from a victimology perspective:

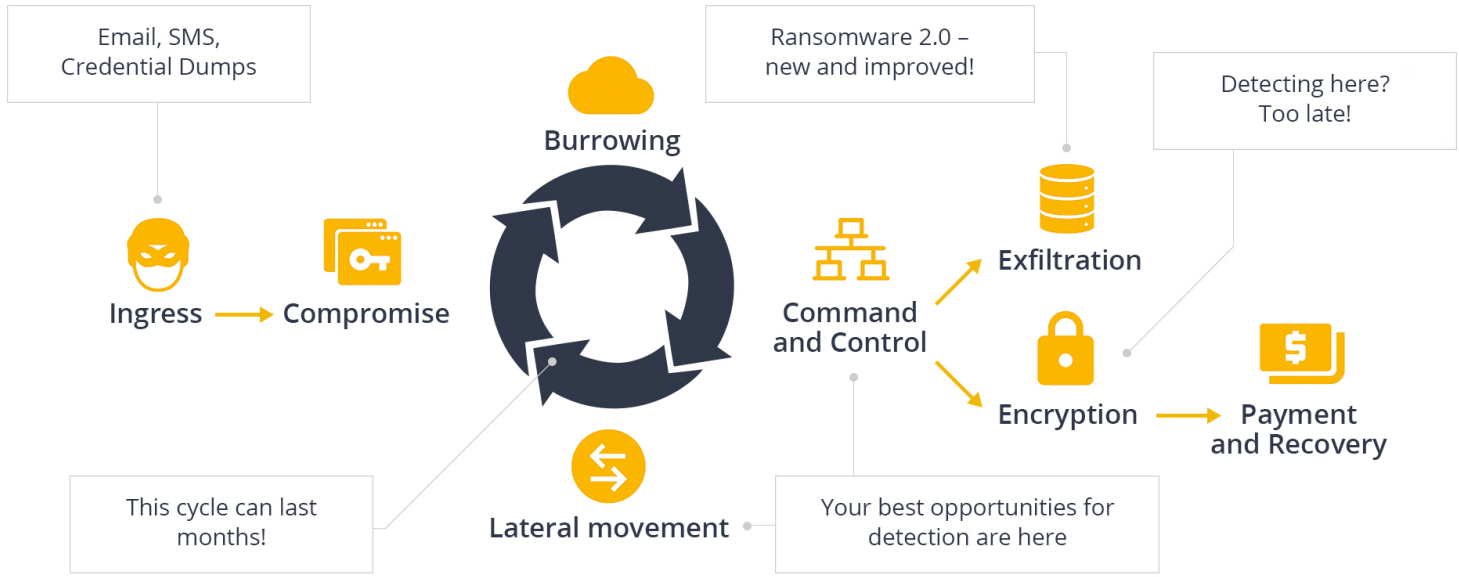
- They are **shifting away from "big-game" hunting** (high-value organizations and/or those that provide critical services generating high-profile incidents) towards mid-sized victims to reduce scrutiny, especially in the US.
- The most relevant **vectors of compromise** remain to be phishing, stolen or brute-forced remote access credentials in exposed assets (such as RDP), and exploiting vulnerabilities in existing enterprise services.
- Most **ransomware attacks are opportunistic rather than targeted** although some indicators are used for attack evaluation, such as maturity of security controls or annual revenue (publicly available). Well-known customers of cyber-insurance providers are also likely to pay the ransom.
- They are heavily **targeting the cloud** by exploiting known vulnerabilities, virtual machine software, or orchestration software. They are actively improving their capabilities against existing Application Programming Interfaces (APIs) with a special focus in data backup and storage systems. Some of those systems are laterally attacked once trusted on-premise devices are compromised.
- They are heavily **targeting managed service providers** because they have a massive, widespread and trusted access into client organizations. Additionally, they have been focusing on software supply chain because they can heavily scale their attacks with a single point of compromise in many customers using the same product.
- They have been **learning how industrial processes work** so that they can start developing code to disrupt critical business processes.

We strongly suggest Information Security professionals to take a deep look into the latests insights provided by CheckPoint and Bryan Krebs about how Ransomware groups internally operate thanks to the leak of the internal chats of the "*Conti*" threat actor.

Tactical Understanding, Investigation, and Response

Following Sun Tzu's wise advice of "knowing your enemy and knowing yourself", leads us to understanding threat actors' modus-operandi, also known as Tactics, Tools and Procedures (TTPs) which reflects their behavior and how they operate.

Anatomy of a Ransomware Attack



REFERENCE: GARTNER

1. Ingress: Identifying exposed assets, vulnerable systems either corporate users' phishing in order to have initial access to internal or cloud asset to start the breach.
2. Compromise: Scanning systems, abuse of internal vulnerabilities, lateral movement to different critical assets including Active Directory, Backup Servers and Central Management Platforms.
3. Burrowing/Lateral Movements: Slipping deeper into the organization systems trying to land into the most relevant systems that host the data (live or in backups) and remarkable management systems including Active Directory and Centralized Management Tools.
4. Command & Control: Remotely management of compromised systems during cyberattack operations.

5. Encryption: Detonation of the ransomware to encrypt the data.
6. Extortion: Asking for a payment in order for getting access to the tool or key that allows to recover data and avoiding it to be leaked online.

In order to respond and investigate ransomware threats, we can consider the following activities:
1. Research and Investigate Threat Landscape Using Threat Intelligence
- Look for active groups/campaigns and their corresponding TTPs/IoCs
- Find IABs selling access to us/third parties in dark markets

2. Attack Surface Identification through Active/Passive Internet Monitoring Platforms
- Identify exploitable systems
- Search for exposed RDP/VPNs and login pages to administrative portals

3. Threat Hunting in Threat Intel Resources and Internal Tools
- Identify phishing attempts against our users
- Search for specific IoC/TTPs in our SIEM/Log platforms

4. Triage/Investigation
- Drill-down specific alerts such as brute-force attempts, lateral-movements, active-directory or backup server anomalies

5. Threat Actor/Leaks Investigation
- Intel collection fro, deep/darkweb forums or leaks from groups
- Search for potential leaked documents in Ransomware sites

6. Follow the Money
- Cryptocurrency wallet and transactions analysis

Relevant OSINT Tools & Data Integrations for Investigations

Maltego provides a wide range of useful data integrations applicable to ransomware investigations from different perspectives and relevant to different teams/functions, including Continuous Monitoring, Threat Hunting, Incident Response, Threat Intelligence and Digital Forensics.

Attack Surface Reduction & Offender activity

Before an incident happens, we can use both Shodan and Greynoise, combined with the NIST NVD vulnerability database and our organization IP ranges, to identify assets exposed to the vulnerabilities abused by threat actors for initial access and obtain some intelligence of the IP addresses scanning and exploiting them.

Greynoise

Query basic IP information such as the owners and its internet scanning activity in the last 90 days. LEARN MORE ›

Shodan

Gain access to intelligence about the global IoT and infrastructure data. LEARN MORE ›

National Vulnerability Database

Discover context and insights of CVEs, CPEs, and CWEs for vulnerability and threat exposure assessment. LEARN MORE ›

Operational Threat Intelligence

Information about ongoing campaigns and their corresponding TTPs/IoCs is needed as part of our defender's strategy to improve our protection and intelligence, performing threat hunting, or during the response of an ongoing incident.

Several in-house and community-based Threat Intelligence Plataforms can provide us access to mentioned information including MISP, OpenCTI, Alienvault OTX, and VirusTotal. STIX2 Utilities would help them to properly structure and link operational information through a standard ontology.

MISP

Query MISP threat sharing instances and other MISP events, attributes, objects, tags, and galaxies. LEARN MORE ›

Alienvault OTX

Access threats, software targeted, and related indicators of compromise used for threat detection. LEARN MORE ›

OpenCTI

Query and explore threat intelligence data from OpenCTI instances using STIX2 Entities. LEARN MORE ›

VirusTotal Public API

Leverage 15 years of malicious sightings to enrich your organization's malware observations and logs. LEARN MORE ›

VirusTotal Premium API

Leverage 15 years of malicious sightings to enrich your organization's malware observations and log. LEARN MORE ›

STIX2 Utilities

Leverage the 40 object types adapted from STIX into the standard Maltego ontology in your investigations. LEARN MORE ›

Threat Hunting & Breach Investigations

Operational intelligence (IoCs/TTPs) collected can be searched over our internal datasets including logs collected from many different platforms including firewalls, proxies, intrusion detection, endpoint security, application logs, etc.

Our Splunk integration helps the analysts to identify potential sources of compromise or even drill down to investigate them, such as lateral movement analysis, critical assets anomalous activities (active directory, backup servers), etc.

Splunk

Cross-reference IP Addresses, domains, hashes, URLs, and other IOCs with internal intelligence. LEARN MORE ›

Deeply Investigating Threat Actors, Leaks & Attribution

As part of our threat landscape profiling or during ongoing threats or incidents, it might be necessary to investigate specific Threat Actors or groups that might be targeting our organization.

Maltego provides access to different threat intelligence providers such as HYAS, Intel471, Flashpoint, RecordedFuture and Silobreaker that generate their own intelligence reports and process data (including that of deep & dark web) that can be queried and correlated in Maltego. This will definitively help us understand and visualize the threat as well as support the attribution process and even identification of potential data leaks.

HYAS Insight

Fingerprint events, actors, and infrastructure with in-depth IOCs data. LEARN MORE ›

Intel 471

Get Adversary, Malware, and Vulnerability Intelligence to support security operation teams. LEARN MORE ›

Flashpoint

Search illicit online communities for fraudulent activities, malicious actors, and other threat intel. LEARN MORE ›

Silobreaker

Tap into deep & dark web for investigations, and enrichment of malware, threat actors, TTPs, and more. LEARN MORE ›

Recorded Future

Gain full picture of threat actors, including known exploit kits, vulnerabilities, or other TTPs. LEARN MORE ›

Infrastructure Investigations

Some of the IoCs provided by cyberthreat intelligence or obtained by our incident response and digital forensic teams include threat actor infrastructure that we can map and track to identify its evolution and other assets related but not actively used yet.

Maltego integrates Farsight Security and WhoisXML API that will support our infrastructure investigations to identify and un-derstand the domains and IP addresses with useful historical information.

Maltego Standard Transforms

Cross-reference IP Addresses, domains, hashes, URLs, and other IOCs with internal intelligence. LEARN MORE ›

Farsight DNSDB

Cross-reference IP Addresses, domains, hashes, URLs, and other IOCs with internal intelligence. LEARN MORE ›

WhoisXML API

Cross-reference IP Addresses, domains, hashes, URLs, and other IOCs with internal intelligence. LEARN MORE ›

Follow-the-Money: Ransom Payments

In some cases, the ransomware victims decide to pay the ransom to the criminal group. In other cases, we want to investigate the activity linked to the cryptocurrency wallets associated with threat actors.

Maltego enables us to identify incoming and outcoming transactions in the Blockchain through data integrations such as Tatum and Ciphertrace, the latter even providing us intelligence information about attribution, use of obfuscation mechanisms (mixers), and maliciousness scoring.

Tatum Blockchain Explorer

Explore and trace transactions on various blockchains such as BTC, ETH, LTC, BCH, and DGE. LEARN MORE ›

Ciphertrace

Access cryptocurrency tracing information for Bitcoin, Ethereum, Bitcoin Cash, and Litecoin. LEARN MORE ›

Start Investigating Ransomware Threats Efficiently!

Link analysis tools, such as Maltego, are built and designed to be a centralized interface to query disparate data sources and aggregate data relationships into visualizations. This enables investigators to:

- Integrate all data in one interface with one click, thereby reducing time and frustration spent on going back-and-forth between different interfaces
- Visually finding connections in seemingly disparate datasets automatically, thereby significantly speeding up investigations
- Collaborate effectively with internal and external stakeholders to provide greater visibility on unknown threats, thereby building upon insights for faster remediation

Maltego is built around graphs, which is fully suited to represent cryptocurrency transactions, especially a great number of them. With its various functionalities to browse, manipulate, and represent graphs, Maltego offers a unified interface in which analysts can interrogate different tools and obtain a clear and informed vision of the transactions being carried on.

At Maltego, the integration of all types of data sources and solutions in a single interface is a central theme of our solution for cybercriminal investigations. If you would like to learn more about Maltego and its capabilities, **get in touch with us**!

MALTEGO

Maltego is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable. With Maltego, you can easily mine data from dispersed sources, automatically merge matching information in one graph, and visually map it to explore your data landscape. Maltego offers the ability to easily connect data and functionalities from diverse sources using Transforms. Via the Transform Hub, you can connect data from over 30 data partners, a variety of public sources (OSINT) as well as your own data. Our different Desktop Client versions, data sources, and server solutions enable you to tailor Maltego to your specific needs in terms of data access, functionalities, and security requirements.

For more information, please visit
maltego.com