

# Talking to RATs: Assessing Corporate Risk by Analyzing Remote Access Trojan Infections

By Insikt Group



*Recorded Future analyzed network communications relating to a selection of RAT command-and-control servers across several malware families in order to profile targeted victim organizations and sectors. This report is based on data sourced from the Recorded Future® Platform, VirusTotal, Farsight DNS, Shodan, GreyNoise, and other OSINT techniques.*

*This report will be of most value to network defenders and corporate risk professionals within companies concerned about the risk posed by their third-party supply chain. To learn more about how to leverage Recorded Future for monitoring and investigating third-party risk, read about [our new Third-Party Risk offering](#). This assessment takes advantage of the data behind our new network traffic analysis risk rules for third-party risk to generate actionable insights.*

## Executive Summary

Remote access trojans (RATs) on a corporate system may serve as a key pivot point to access information laterally within an enterprise network. By analyzing network metadata, Recorded Future analysts were able to identify RAT command-and-control (C2) servers, and more crucially, which corporate networks were communicating to those controllers. This approach allows Recorded Future to provide insight about third-party organizations that our clients may rely upon, enabling a better understanding of potential third-party risk to their own data.

Insikt Group used the joint Recorded Future and Shodan Malware Hunter project and the Recorded Future Platform to identify active malware controllers for 14 malware families between December 2, 2018 and January 9, 2019. We then focused our analysis on a subset of malware — Emotet, Xtreme RAT, and ZeroAccess — to profile RAT communications from third-party organizations to the controllers.

## Key Judgments

- The majority of Emotet controllers resolved to IPs in Latin American countries.
- A significant proportion of infected Emotet hosts were based in Latin America, corroborating community observations of a surge in late-2018 Emotet activity targeting South American entities. Infected hosts include organizations in the automotive, finance, energy, construction, retail and entertainment, logistics, and technology sectors.
- Infected Xtreme RAT hosts were identified within:
  - A video game company and a utilities company in Europe
  - Middle Eastern, South Asian, and East Asian telecommunications companies
  - An industrial conglomerate and an IT company in East Asia



### What Do RATs Do?

Across the world, public and private companies continue to suffer from increasingly frequent and complex cyberattacks and data breaches.



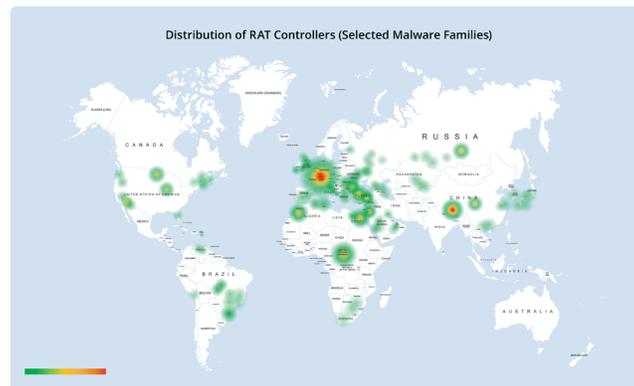
**557 incidents**  
between September 1, 2017  
and August 31, 2018 in the U.K. alone



Attackers sometimes use RATs to illicitly gain control of a host device and conduct activity such as keylogging, file extraction, the recording of host audio and video, and more.

 <p><b>Emotet</b></p> <p>An advanced, modular banking trojan with worm-like characteristics that was initially designed to steal financial data, but is now more commonly used to download other malware programs.</p>	 <p><b>Xtreme RAT</b></p> <p>A free-to-use RAT comparable in capability to many commercially available RATs, which has attracted a wide range of users, from hacking novices to cybercriminals and suspected APTs targeting national defense networks. Xtreme RAT source code has been leaked online, enabling attackers to develop code modifications to evade AV.</p>	 <p><b>ZeroAccess</b></p> <p>A multi-purpose RAT that is difficult to detect due to its advanced rootkit. ZeroAccess was frequently used for cryptomining and other financial fraud. Advanced ZeroAccess features include the ability to utilize domain generation algorithms (DGA) and peer-to-peer connectivity for C2 communications.</p>
--	---	---

### Where Are RATs Being Used?



Recorded Future heatmap showing Xtreme RAT controllers active during the research period, as detected using the Recorded Future and Shodan Malware Hunter project. (Source: Recorded Future)

### What Can You Do About It?

RATs continue to pose significant threats to governments and companies around the globe. Using Recorded Future's Third-Party Risk module, clients can identify and analyze malware communications in their networks and implement appropriate defenses in a timely fashion.

## Background

Public and private organizations all over the world continue to experience digital intrusions with news of large breaches being almost a daily occurrence. In their 2018 annual review, the [U.K's NCSC reported that they had directly handled 557 incidents](#) between September 1, 2017 and August 31, 2018 highlighting the scale of the problem just in the U.K.

Often, attacks utilize RATs, which enable attackers to illicitly gain control of a host device. RATs are a feature-rich software generally used by adversaries to conduct activity such as keylogging, file extraction, recording host audio and video, [and more](#).

A significant proportion of these attacks are carried out using commodity RATs, such as DarkTrack RAT, Xtreme RAT, or ZeroAccess, with attacker motivations ranging from financial gain to gaining credibility within hacking communities. Many hacking forum administrators will stipulate that new members provide evidence of their “ability” in order to be accepted into the forum, so the relatively low-level technical knowledge required to use commodity RATs, along with extensive online documentation, makes them a highly attractive proposition for inexperienced hackers.

At the other end of the spectrum are state-backed advanced persistent threat (APTs) groups and advanced criminal groups who may conduct malware campaigns with greater sophistication in order to achieve their operational outcomes. APTs continue to use RATs because they are easy to configure, modify, and use. This combined with their relative effectiveness against antivirus software and the potential for hindering attribution by “hiding in the noise” ensures RATs continue to be used by APTs and cybercriminals.

Cybercriminals have often been forced to innovate in developing tooling and malware to support their usually financially motivated objectives. As RATs and other malware used by cybercriminals are disrupted by law enforcement action or their methods are neutered by coordinated industry initiatives, a change in methodology or even business model is sometimes forced. This has been the case with the actors behind Emotet.

Emotet has evolved from a banking trojan targeting European banking customers to a modularized malware deployment platform with [several](#) high-profile [campaigns](#) noted in 2018. Emotet, as a self-propagating trojan, is a particularly virulent piece of malware that exhibits network worm-like characteristics, enabling it to build up a considerable botnet of infected victims.

## Analytic Approach

Recorded Future researchers identified a variety of RAT and Emotet controllers derived from threat lists in the Recorded Future platform and used network metadata to identify victim communications with the RAT C2 IPs. The threat lists included data from:

1. Recorded Future's jointly-developed [Malware Hunter](#)<sup>1</sup> capability with Shodan
2. The Abuse.ch Feodo malware family (also known as Dridex or Emotet/Heodo) blocklist

*Editor's Note: Due to technological limitations of the collection mechanism, the number of C2s identified using Malware Hunter is not reflective of the true number of C2s present globally for each analyzed malware family in this research. Therefore, this analysis is focused on the methodology of identifying infected clients using Recorded Future to inform third-party risk.*

For the purposes of our research, we searched for active controllers in the December 2, 2018 to January 8, 2019 time frame for the following malware families:

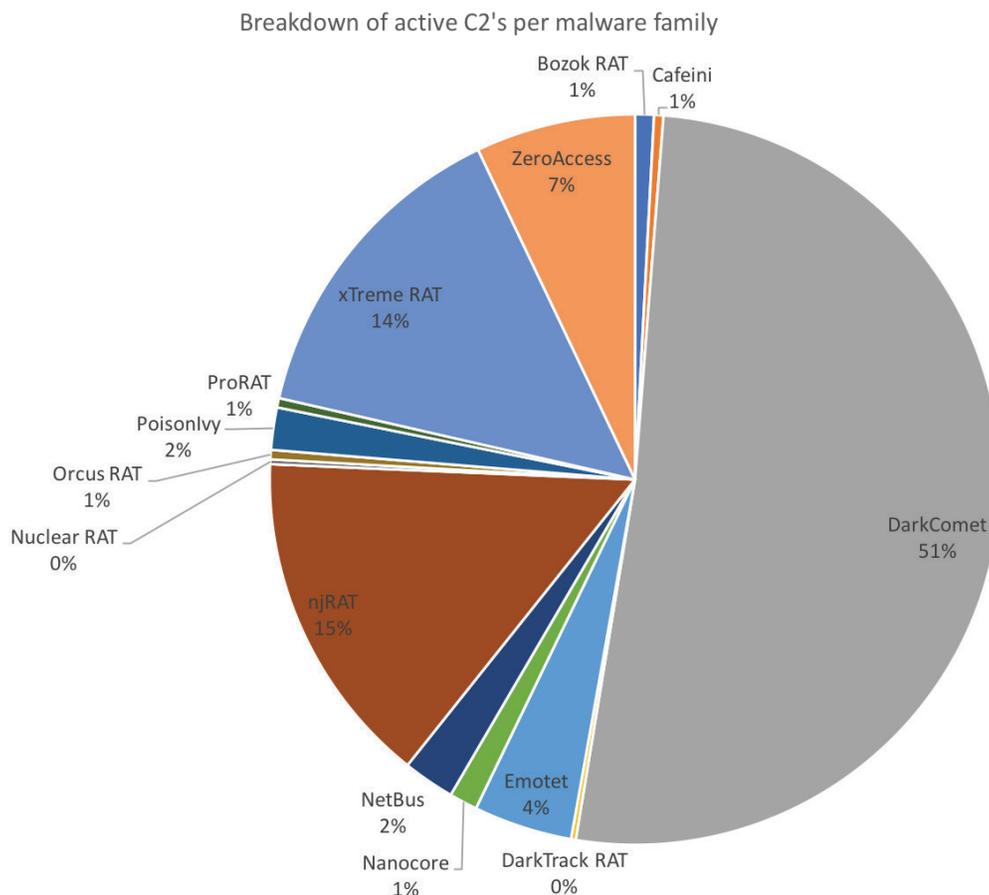
- Bozok RAT
- Nanocore
- PoisonIvy
- Cafeini
- NetBus
- ProRAT
- DarkComet

---

<sup>1</sup> For more detail on the capability, please refer to the [Recorded Future white paper on proactive threat identification](#).

- njRAT
- Xtreme RAT
- DarkTrack RAT
- Nuclear RAT
- ZeroAccess
- Emotet
- Orcus RAT

We then analyzed network communications for a subset of these controllers from victim organizations. Filtering was conducted to avoid identifying organizations that provide internet hosting services to other organizations as being directly victimized, and internet scanners were omitted where identifiable. This analysis is based upon the observation of connections made in a specific manner to servers identified as malicious, and the possibility exists that researchers or others that are not in fact victims have made such connections.

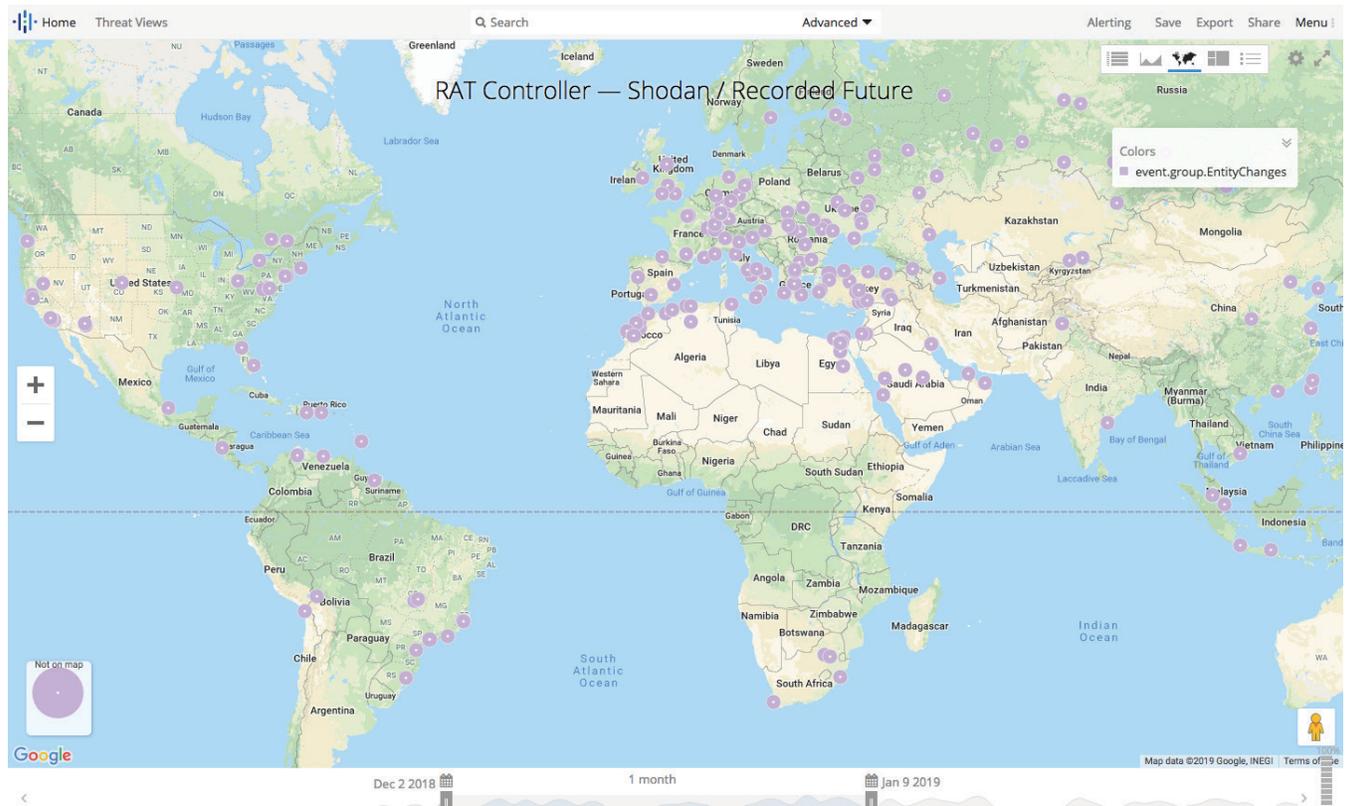


Breakdown of active C2s per malware family identified (total sample size of C2s detected: 481).

We focused our analysis on Emotet, Xtreme RAT, and ZeroAccess controllers to profile RAT communications with probable infected hosts within commercial organizations' infrastructure.

## Recorded Future's Third-Party Risk Module

Following the launch of Recorded Future's [Third-Party Risk module](#), we have integrated additional features that will enable enterprises to assess cyber risk posed by companies in their supply chain, partners, and themselves. Third-Party Risk enables you to monitor your third-party ecosystem's health, investigate risks posed by companies, and alert on changes in the threat environments of companies of interest to you. The analysis in this report was conducted using the same data sources we are using to inform third-party risk factors and metrics in our new module, especially our network traffic analysis risk rules.



Global distribution of RAT C2s identified using Recorded Future and Shodan's Malware Hunter project and the Abuse.ch Feodo blacklist. (Source: Recorded Future)

## Threat Analysis

### Emotet

Emotet is an advanced, modular banking trojan that primarily functions as a downloader or dropper of other banking trojans. Emotet was initially designed to steal financial data; however, it is now mostly used as a downloader for other malware such as Trickbot and Qakbot. Emotet uses C2 servers to receive updates as well as download and install any additional malware. Emotet operators tend to not be selective about targeting a specific industry or region, instead spreading without discretion, revealing that the malware operators appear more interested in large volumes of infection to generate profit.

Emotet was originally identified as a new banking trojan in 2014, and is often referred to as Geodo or Feodo. The malware was the product of natural evolution from the Feodo (sometimes called Cridex or Bugat) banking trojan, which spawned other offspring. In the past 12 months, however, it evolved from a standalone threat into a distributor of other trojans, with [numerous](#) large campaigns taking place over the summer of 2018. The malware is unique in that it employs a litany of open source libraries and code, enough to [title](#) a folder in its code directory as “Open Source.” A number of Emotet modules incorporate utilities developed by Nirsoft to scrape and gather passwords on the victim machine.

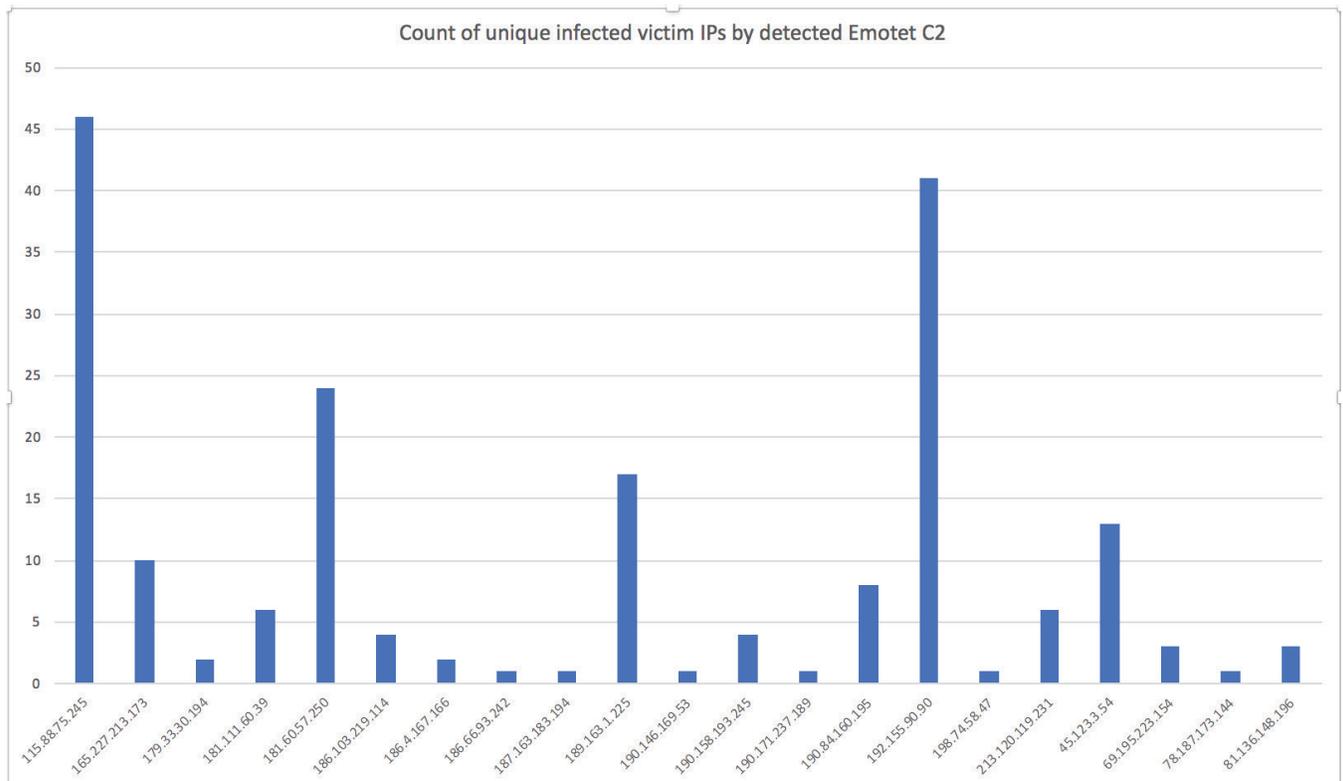
Emotet has recently been acting as a spam-sending malware that infects target systems to then load other malware families onto the host. The infected hosts that distribute spam and occasionally act as proxies for the C2 servers are a decentralized network, making it difficult for defenders to block at their perimeter.

Reporting has revealed that the operators of Emotet are likely maintaining at least [two Emotet infrastructure setups in parallel](#), likely to aid redundancy and to make it harder for coordinated takedown by law enforcement.

### Emotet: Evaluating Third-Party Risk Using Network Metadata

During our research, we identified 26 organizations with hosts infected with Emotet. These organizations were spread across a variety of industries, including:

- Automotive
- Finance and banking
- Energy
- Medical device manufacturing
- Construction
- Retail and entertainment
- Logistics, commercial services, and supplies
- IT
- Utilities



The chart above shows us the breakdown of infected hosts communicating with identified Emotet controllers. Two controllers stand out, with over 40 infected hosts observed communicating with them: South Korean IP 115.88.75[.]245 and U.S. IP 192.155.90[.]90.

Emotet C2 IP	Country	ISP
181.111.60[.]39	Argentina	Telecom Argentina S.A.
190.171.237[.]189	Bolivia	COTAS LTDA.
186.103.219[.]114	Chile	Telefonica Empresas
179.33.30[.]194	Colombia	COLOMBIA TELECOMUNICACIONES S.A. ESP
181.60.57[.]250	Colombia	Telmex Colombia S.A.
190.146.169[.]53	Colombia	Telmex Colombia S.A.
190.158.193[.]245	Colombia	Telmex Colombia S.A.
190.84.160[.]195	Colombia	Telmex Colombia S.A.
186.4.167[.]166	Ecuador	Telconet S.A
186.66.93[.]242	Ecuador	Satnet
45.123.3[.]54	India	Blue Lotus Support Services Pvt Ltd
115.88.75[.]245	South Korea	LG DACOM Corporation
187.163.183[.]194	Mexico	Axtel S.A.B. de C.V.
189.163.1[.]225	Mexico	Uninet S.A. de C.V.
78.187.173[.]144	Turkey	Turk Telekom
213.120.119[.]231	United Kingdom	British Telecommunications PLC
81.136.148[.]196	United Kingdom	British Telecommunications PLC
165.227.213[.]173	United States	DigitalOcean LLC
192.155.90[.]90	United States	Linode LLC
198.74.58[.]47	United States	Linode LLC
69.195.223[.]154	United States	Elite Hosts Inc.

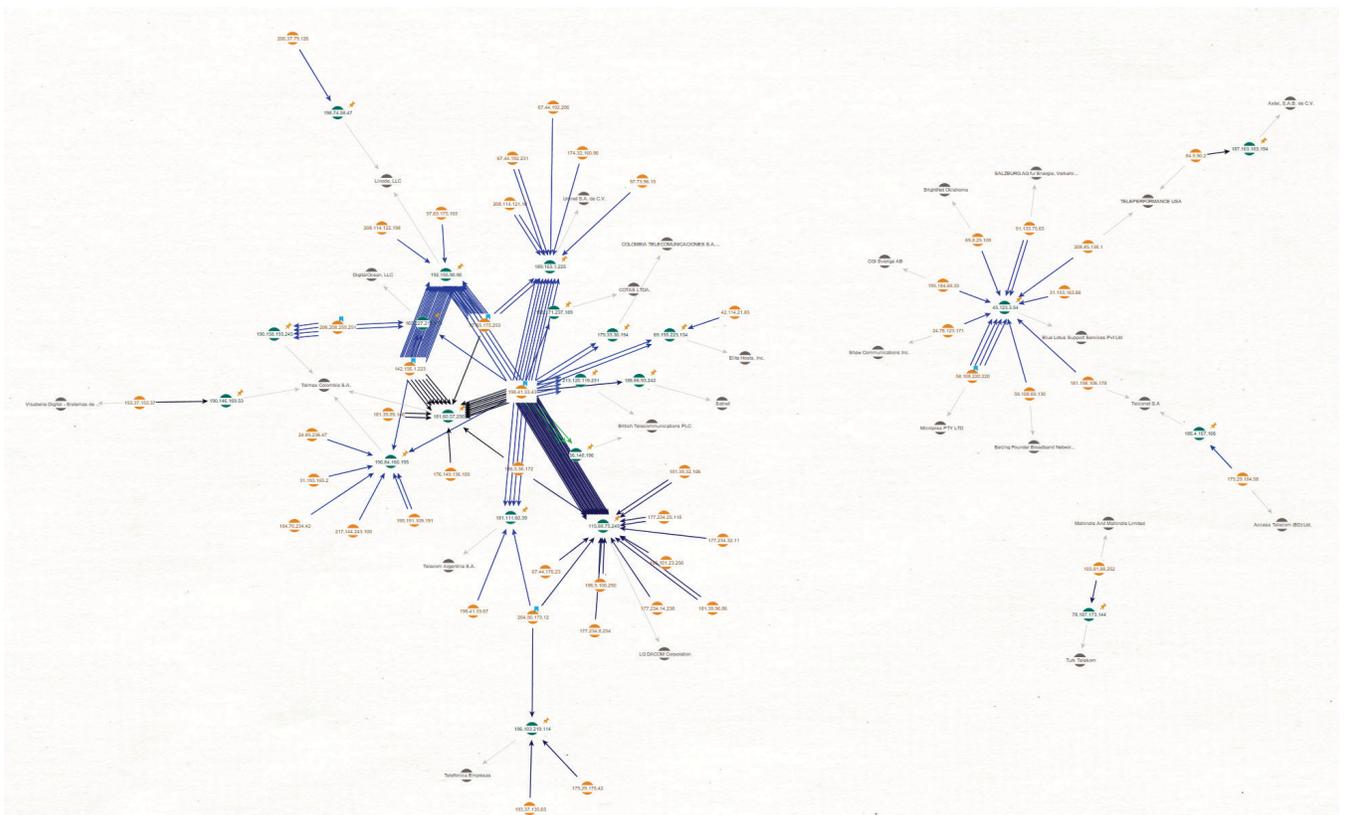
*Emotet C2s identified with active corporate victim infections between December 2, 2018 and January 8, 2019.*

The table above identifies the IP address, country, and internet service provider (ISP) of each Emotet C2 server analyzed in depth by Recorded Future.

*Editor's Note: ISPs provide internet access to customers, and may not be directly in control of the equipment and systems in use at any specific IP address within a netblock assigned to the ISP.*

One of the most active Emotet C2s, based on number of unique corporate victims communicating with it in our research data, was South Korean IP 115.88.75[.]245. Based on our new algorithm that has been developed into a new risk rule for clients using the Recorded Future platform, IP addresses resolving to at least four different infected companies were detected communicating with the C2. Three of the infected companies were located in Latin America, [which has recently experienced a surge in Emotet infections](#) due to a slightly modified Emotet propagation methodology being employed. Two of the detected victims were financial companies in Mexico and Ecuador, with the third being a Chilean industrial conglomerate. The remaining corporate victim was a Canadian medical device manufacturing company.

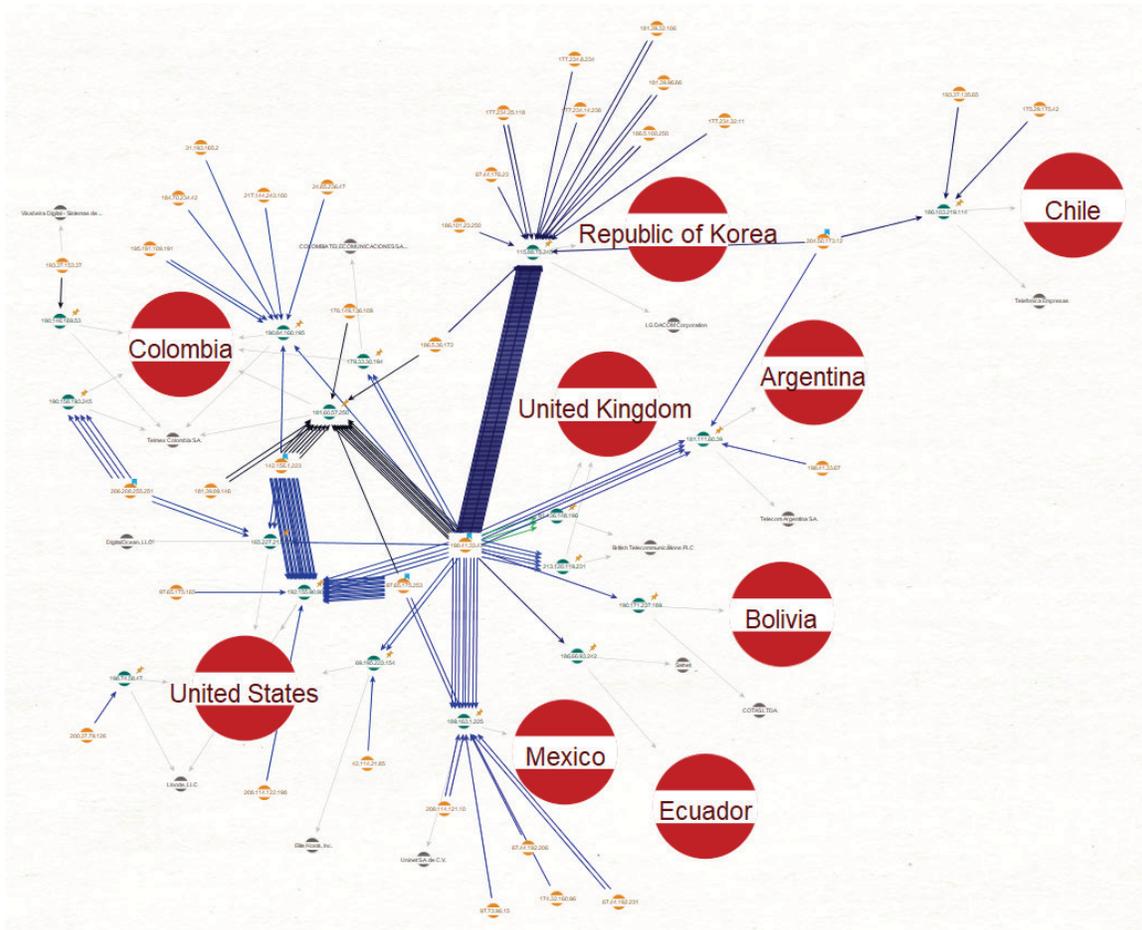
The South Korean C2 IP did not have a domain resolving to it at the time of this research, but VirusTotal data indicates that connections with the IP address, explicitly noted as the host in the URL, were made to it from infected victims. We identified several malicious Microsoft Word documents containing obfuscated VBA<sup>2</sup> code as macros designed to launch PowerShell, which in turn would retrieve and run an Emotet payload from the South Korean C2.



*Clustering of Emotet C2s and communicating victim organizations detected using Recorded Future third-party risk analytics and network traffic analysis risk rules.*

<sup>2</sup> Visual Basic for Applications is an implementation of Microsoft's Visual Basic 6 programming language and is used in Microsoft Office products, such as Excel, to develop macros.

Further analysis of the Emotet C2s and the victim organization IPs revealed that there were several distinct groupings of activity as shown in the Maltego graph above. The highly active South Korean C2, detailed previously resolving to LG DACOM Corporation, sat within a highly interconnected cluster of activity shown on the left-hand side of the graph. This cluster centered on 17 detected Emotet C2s mostly hosted on infrastructure resolving to telecommunications service providers and hosting providers based in Latin America. The targeted organizations in the cluster of activity were based around the world, with a significant proportion of victim organizations based in Latin America and Europe.



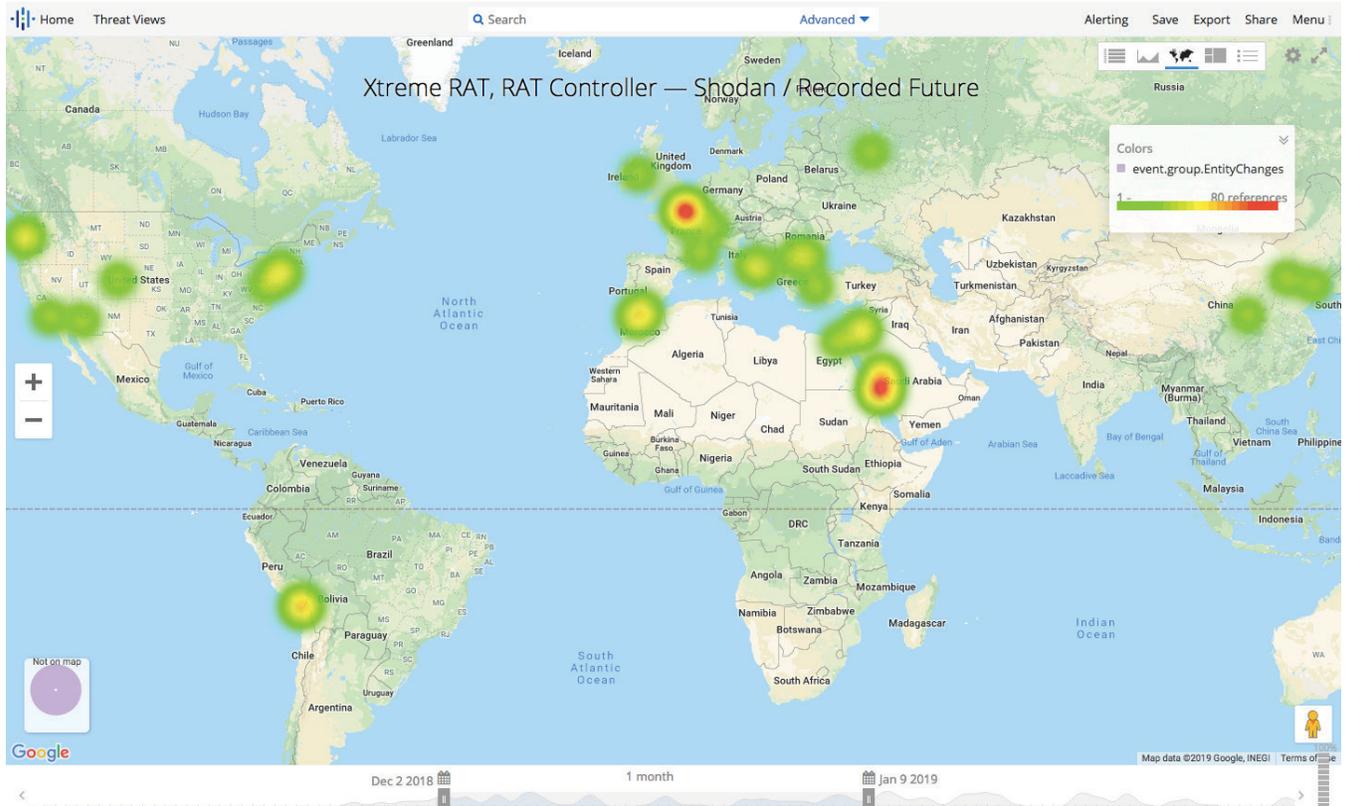
Primary cluster of Emotet activity with the majority of C2s located in the Latin American IP space.

The second largest cluster of activity we observed centered on an Emotet controller hosted on Indian IP 45.123.3[.]54, which resolved to Blue Lotus Support Services in India. The C2 hostname pointing to this IP was campus.miim.ac[.]in, which corresponds to the Marian International Institute of Management, a university in Kerala, India. Our analysis revealed ongoing Emotet infections pertaining to this C2 at the following companies:

- A Japanese machine manufacturer
- A Chinese technology conglomerate
- An Ecuadorian bank and a U.S. financial consulting firm
- An Austrian energy supplier
- Canadian and Australian cable TV providers

### **Xtreme RAT**

Xtreme RAT is a commodity RAT that was first publicly sighted in 2010. The RAT is available for free and the source code for it has been leaked, enabling attackers to modify it freely to evade network defenses. Although it has been around for almost a decade and usage appears to be lower than previous years, it is still a potent trojan that [has been widely reported as being](#) used in targeted attacks and cybercrime activity. This RAT utilizes a client-server system that was defined by the author in a [reverse of the usual scheme](#). The “server” part of the malware is installed on the victim’s computer, and the victim’s “server” thus connects with the “client,” which is in reality a controller operated on one or more remote C2 systems.



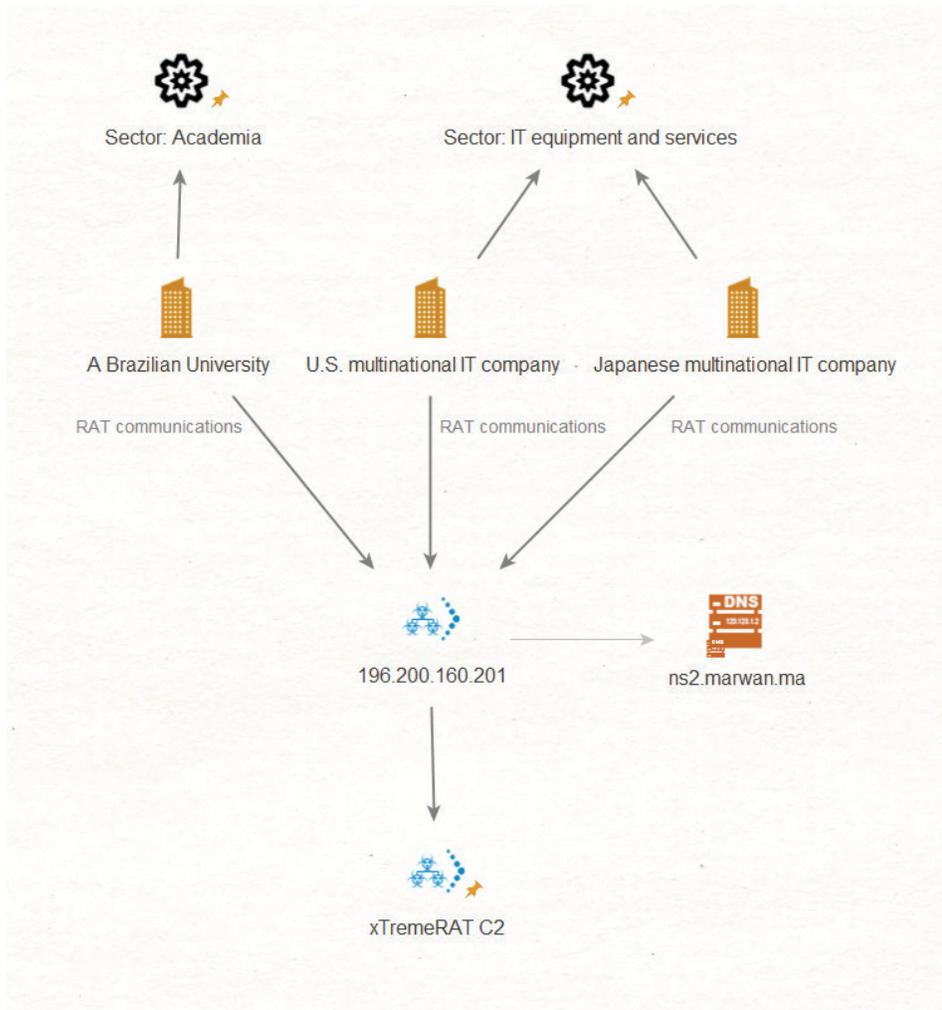
Recorded Future heatmap showing Xtreme RAT controllers active during the research period as detected using the Recorded Future and Shodan Malware Hunter project. (Source: Recorded Future)

### Xtreme RAT: Evaluating Third-Party Risk Using Network Metadata

We deployed our new Third-Party Risk module to identify communication nodes with active Xtreme RAT controllers that we observed between December 8, 2018 and January 2, 2019. Once again, we found corporate IPs communicating with the Xtreme RAT controllers in a manner that indicated probable infection.

Xtreme RAT C2 IP	Country	Registrant/Organization
101.132.69[.178]	China	Hangzhou Alibaba Advertising Co.,Ltd.
116.62.60[.1109]	China	Hangzhou Alibaba Advertising Co.,Ltd.
212.46.104[.1104]	Germany	HKN GmbH
196.200.160[.1201]	Morocco	CNRST (Centre National pour la Recherche Scientifique et Technique)
198.255.100[.174]	United States	FDCServers
192.240.110[.198]	United States	FDCServers

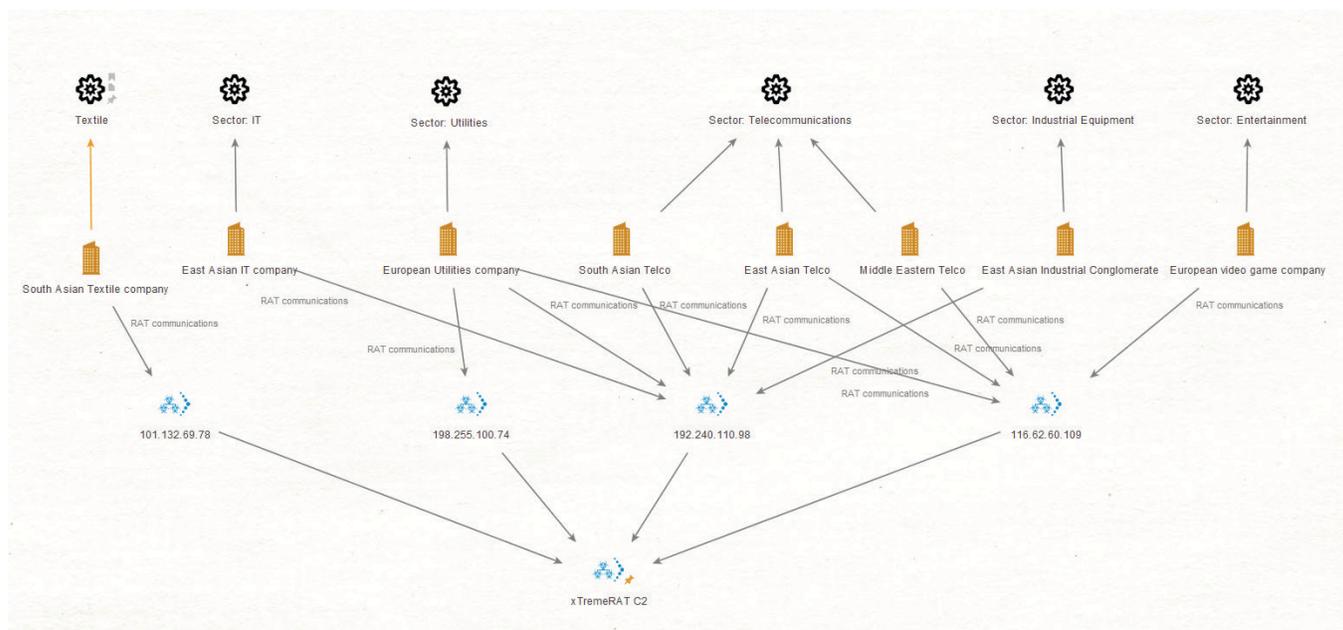
Three unique victims were found communicating with a Moroccan Xtreme RAT C2 hosted on 196.200.160[.]20,1 which resolved to hostname ns2.marwan.ma. The IP is registered to the Centre National pour la Recherche Scientifique et Technique (CNRST), a technical university in Rabat, Morocco. Two of the infected victim devices resolved to infrastructure belonging to U.S. and Japanese multinational IT equipment and services companies. The third victim was a device located at a Brazilian university



*Xtreme RAT controller hosted on a Moroccan university network.*

Hostname test.zzzjpt[.]com was updated to point at Chinese IP 116.62.60[.]109 on December 16, 2018 and continued to resolve to that IP until at least January 5, 2019. In this time frame, the IP was designated as an Xtreme RAT C2. This controller, along with two other Xtreme RAT C2s hosted on U.S. FDCServer infrastructure (192.240.110[.]98 and 198.255.100[.]74), were observed receiving Xtreme RAT network communications from several infected hosts within an European utilities company. Additional victim organizations that were observed communicating with these Xtreme RAT C2s were:

- A European video game company
- Middle Eastern, South Asian, and East Asian telecommunications companies
- An East Asian industrial conglomerate
- An East Asian IT company



*Xtreme RAT controllers with overlapping organizational targeting.*

## ZeroAccess Trojan

ZeroAccess was first discovered in 2011, and it utilizes an advanced rootkit to evade detection. As a trojan, it can create a hidden file system and backdoor on a host as well as facilitate the downloading of additional malware onto the host. ZeroAccess can be configured to make use of a domain generation algorithm (DGA) to discover and connect to its C2 servers and may also utilize peer-to-peer connectivity. [Historically, ZeroAccess was deployed using strategic web compromises](#) (SWC) and was typically used by cybercriminals in order to generate illicit funds through pay-per-click advertising mechanisms (click fraud). The malware has also been used to [mine for cryptocurrency](#).

## ZeroAccess: Evaluating Third-Party Risk Using Network Metadata

During our research period, we identified a single instance of a victim organization communicating with a ZeroAccess trojan C2 active on Romanian IP 31.5.229[.]224. The victim organization was an East Asian IT company.

## Outlook

Banking trojans like Emotet and other RATs continue to pose significant ongoing threats to government and company networks around the world. The developers behind Emotet continue to innovate and develop modularized functionality to aid propagation efficacy and evade traditional network defenses, resulting in widespread infection which according to a [US-CERT alert issued in July 2018](#), have cost state, local, tribal, and territorial (SLTT) governments up to \$1 million per incident to remediate.

This research highlights the benefit of being able to identify and track malicious RAT controller network infrastructure to inform the security posture of your enterprise. Clients can use Recorded Future's [Third-Party Risk module](#) by observing related risk rules triggered within our platform. With Third-Party Risk, the same data we used to identify and analyze malware communications in this assessment trigger risk rules and raise an alert when a company in a client's third-party risk watch list demonstrate similar activity.

#### Triggered Risk Rules

---

**Infected Hosts Recently Communicating with C&C Server** • 33 sightings

Active command and control communication on uncommon ports related to malware from 2 infected hosts: [REDACTED]

[REDACTED] 1 related malware: XtremeRAT trojan. Last observed on Jan 8, 2019.

*Third-party risk network traffic analysis risk rule showing high-severity risk associated with Xtreme RAT communications observed on a company's infrastructure.*

As we continue to develop additional coverage of RAT controllers, we will automatically add these signatures so they trigger third-party risk rules in the Recorded Future platform when we observe corporate network infrastructure communicating with these controllers.

## Network Defense Recommendations

Recorded Future recommends organizations conduct proactive threat hunting and implement the following mitigations when defending against illicit RAT activity:

- Use Recorded Future's API to import indicators listed in this report (Appendix A) into your endpoint detection and response (EDR) platform.
- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking illicit connection attempts from — the external IP addresses and domains listed in Appendix A.
- Monitor endpoint traffic to alert and block connections to indicators in Appendix A.

## Appendix A — [Indicators of Compromise](#)

Complete list of malware controller IPs identified during research that were active between December 2, 2018 and January 8, 2019 can be found in the attached csv and from the [Insikt Group GitHub repository](#).

### About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.