

Insider Threats to Financial Services: Uncovering Evidence With External Intelligence

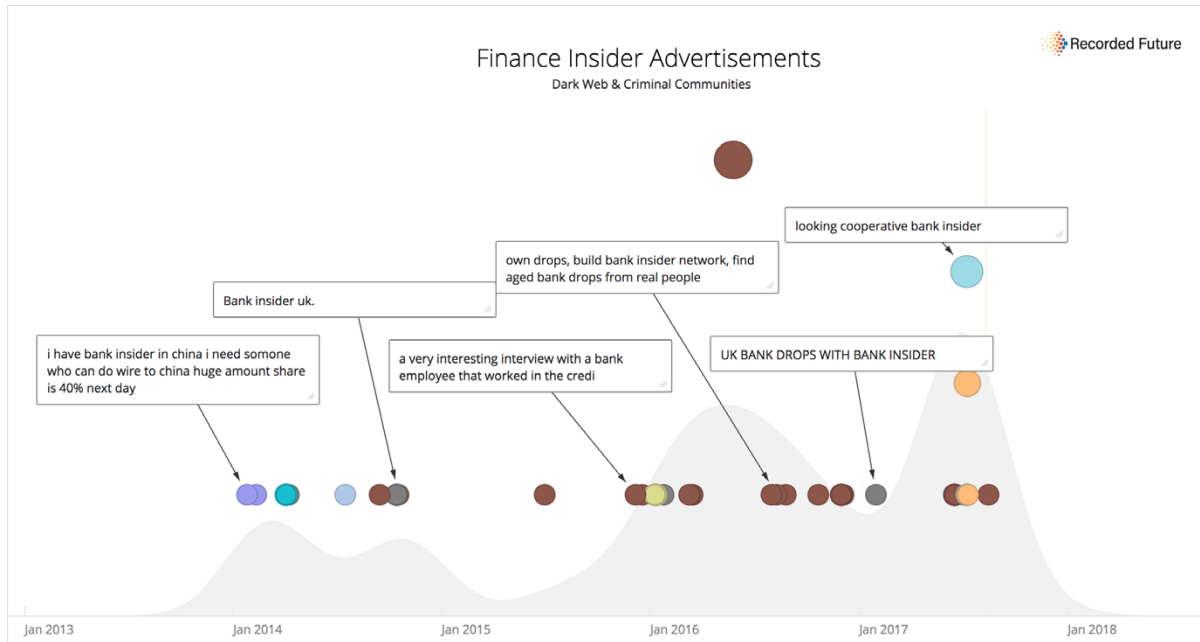
By John Wetzel

Threat Intelligence Analyst

Key Takeaways:

- › Threat actors and insiders are using underground forums and criminal marketplaces to communicate.
- › Malicious insiders often evade security controls because elevated privileges to systems are not managed, not revoked, or missed by internal detection methods.
- › Threat intelligence can detect early indications of insider threats, as well as breaches resulting from their actions.

Insider Threats — An Increasing Concern



Finance insiders increasingly taking to the dark web to advertise their access.

The insider threat is undoubtedly a top security issue today. Once solely the concern of government and defense organizations, risks posed by employees, contractors, or third parties are now clearly on the radar for commercial enterprises. This growing concern may be due to fall out from the Snowden affair and a number of high-profile breaches in 2016. Recent developments in the techniques of threat actors have seen them begin to solicit and recruit insiders on the dark web. Insiders are also advertising their access to the networks and infrastructure of banking or financial service companies.

Today, more companies than ever before are seeking insider threat detection and prevention processes and tools. Research from leading analysts at Forrester revealed that insiders accounted for 39% of data breaches through accidental and malicious misuse of data.

The principle of least privileged asserts:

“ Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job. ”

The challenge here is that networks are organic in their own way. Over time many different types of users have been given access to various servers and other network resources. It's also highly likely that many of those privileges have not been revoked. It's this situation combined with the human nature of users which results in risks from insiders. Further, insiders may evade security controls entirely. Traditional perimeter defenses, like firewalls and intrusion detection systems, are not configured to detect insider behaviors. Even some maturing technologies like Data Loss Prevention and User and Entity Behavior Analytics prove challenging to security teams, as the resulting alerts add to the information overload teams already struggle to manage.


Defining an Insider Threat

Any examination of the risk posed by an insider needs to start with defining the threat. To do this effectively it's important that we eliminate the psychological distance we place between "normal" employees and insiders. Most insiders join an organization with no malicious intent, but motivations to act will likely increase over time or in the wake of a compelling event. Beyond the careless user who poses a risk due to their negligence, insiders may be motivated by money, ego, or conflicting ideology. In some cases employees are being coerced or blackmailed by malicious outsiders.

While it's impossible to exactly profile the motives and methods of every insider, to help understand the likely risks they pose we can broadly assign them three categories:

- › **Negligent** — Employees that may accidentally move or edit corporate data or unwittingly share sensitive information. This kind of accidental disclosure may come in the form of posting information on public-facing websites or social media, sending information to the wrong people, or uploading data to unapproved cloud storage.
- › **Exploited** — Insiders are exploited when an external threat actor uses them to find their way into the corporate network via phishing or malware. Beyond an insider being unwittingly compromised, a network user who has been recruited or coerced could also fall into this category.
- › **Malicious** — These are individuals who act to deliberately access and exfiltrate critical company information. They typically do this to profit from selling the data or access they have. Cases of malicious insiders also include sabotage of facilities, equipment, and IT infrastructure. These cases are the most challenging to identify and can cause some of the greatest harm to an organization.

The State of the Insider Threat

Data Centre ▶ Networks 

Ex-Citibank IT bloke wiped bank's core routers, will now spend 21 months in the clink

Performance review sparks deletion, 110 offices knackered

By Shaun Nichols in San Francisco 27 Jul 2016 at 18:57 SHARE ▼

A former employee of Citibank has been sentenced to 21 months in prison for crippling the bank's internal network.

Lennon Ray Brown was given the nearly two-year jail term – along with a \$77,000 fine – by a Northern Texas District Court this week after he pleaded guilty to one count of intentional damage to a computer.

http://www.theregister.co.uk/2016/07/27/citibank_network_wipe_man_jailed/

Smartphones | Cybersecurity | Innovation | Social Media | Games | Motoring

Technology | CyberSecurity

Sage employee arrested at Heathrow airport for 'insider threat' data breach

■ The 'unauthorised access' reportedly exposed between 200 and 300 major customers.

By Jason Murdock
August 18, 2016 17:05 BST

f t g+ r in



Sage suffered an insider threat breach that left 200-300 of its customers exposed (iStock)

Police in the City of London have arrested an employee of UK technology firm Sage in connection with an ongoing investigation into a recent data breach believed to have impacted between 200 and 300 of its customers.

The arrest of the 32-year-old woman, who remains unnamed at the time of writing, comes only days after the finance and accounting software firm admitted it had suffered "unauthorised access" on its computer systems that left data at risk.

<http://www.ibtimes.co.uk/sage-employee-arrested-heathrow-airport-insider-threat-data-breach-1576809>

ECONOMY | CENTRAL BANKS

Bangladesh Panel Hints at Possible Insider Role in Central Bank Theft

Government panel hands in report on theft of \$81 million from Swift network

By Syed Zain Al-Mahmood

Updated May 30, 2016 8:06 p.m. ET

A Bangladeshi government-appointed committee investigating the theft of \$81 million from the South Asian country's account at the Federal Reserve Bank of New York blamed the Swift interbank messaging service for negligence but also hinted at insider involvement after handing in its final report Monday.

Mohammad Farashuddin, a former central banker who led the committee, said Swift

Most Popular Videos

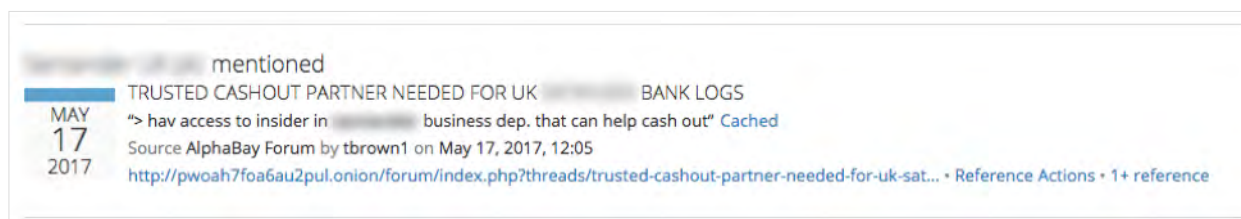
1. Sen. Graham: The 'Skinny' Bill Is a Disaster
2. Dan Neil Drives VW's Atlas



<https://www.wsj.com/articles/bangladesh-panel-hints-at-possible-insider-role-in-central-bank-theft-1464631707>

For good reason, much news coverage of insider threats highlights the risk from espionage and large-scale financial theft. In February 2016, the Bank of Bangladesh issued a statement that criminal hackers had stolen the equivalent of over \$86 million from the bank. Likely using custom malware and insider information, the criminals sent forged SWIFT messages to withdraw funds from the Bank of Bangladesh's account at the U.S. Federal Reserve Bank. In total, the criminals attempted to steal over \$1.1 billion.

Criminal actors recognize insiders as a rich source of both sensitive access and valuable knowledge across industries. According to 2016 research by [Kaspersky Labs and B2B International](#), criminals targeting the telecommunications industry used insiders to penetrate network perimeters and recruit other insiders. Recorded Future has also uncovered examples of finance insiders advertising their access in criminal forums and dark web marketplaces.



Threat actor already has access to bank details but is seeking an insider to withdraw cash.

Criminals may use previously compromised data, such as the Ashley Madison breach, to blackmail telecommunication employees for credentials, information, to propagate spear phishing emails, or recruit other employees for further malfeasance.

Approaches to Securing Against Insider Threats

A survey of more than [500 cybersecurity professionals in 2016](#) revealed that 56% say insider threats have become more frequent in the last 12 months and 42% of organizations expected a budget increase over the next year. It's likely then that enterprises will be seeking out new services and technologies to help to address the risk from insiders.

Insider threat investigations originated from espionage hunts within intelligence agencies. Often, these investigations began from some kind of external indication of insider information, like an adversary developing technology at a faster pace than expected. Once triggered by external information, these investigations searched for insiders who have access to the critical information which was leaked.

Current security technologies aimed at preventing and detecting insider threats are generally focused on managing identity and access, ensuring the right people have access to the right systems. Another capability is the monitoring, recording, and analyzing of user behaviour on internal systems. Even with tools like these correctly configured and deployed, insiders can evade detection, as their actions may fall within the spectrum of expected behaviors. Worse, many insider threat detection efforts may end up generating false positives, contributing to the problem of noise and alert fatigue already experienced by many security teams.

Just as criminal actors utilize betrayal, employees or contractors may seek out criminal actors to help them with the transmission, purchase, or sale of corporate assets and data. While the operational act of goods for money is often conducted via private means, it is possible to identify various indications of insider threat.

The biggest risk associated with uncovering these kinds of indications is to concentrate effort on unproductive sources of intelligence. This issue arises as organizations tend to treat insiders as solely a security problem, which can limit their perspective on external resources. Typically, many businesses will focus first on costly internal detection methods, then monitor external sources only for perceived signs of risk, such as negative sentiment in social media posts.

There are three potential reasons why current approaches are challenging for businesses:

1. Behavioral monitoring is expensive, particularly when you consider how scarce insider threat activity is in comparison to other cyberthreats. Monitoring tools sap precious security resources in both the direct costs to purchase the software, and the human costs of dedicated monitoring. While purchased for live monitoring, these tools frequently become noisy alerting stations or incident response black boxes for evidence retrieval rather than a solution for proactive hunting.
2. Insider threat systems generate significant noise in general, particularly when targeting high-noise sources. Social media monitoring is a high-noise source and, as such, does not always provide the best means for insider threat detection and analysis.
3. The insider threat program itself may become a cause of discontent among your employee base. Exposure of monitoring programs, such as social media monitoring and reporting on employee behaviour, risks creating an enmity between the organization's security policies and an employee's privacy. Increased employee disenfranchisement can ultimately even contribute to potential insider activity.

Combatting insider threats requires fusion between security teams, business teams, and technologies. Using threat intelligence for insider threats is beneficial to detection efforts. Any breached data or access attained by an insider typically seeks a customer for the product of their betrayal. Likewise, criminal actors and nation states continually hunt new avenues for deeper access to internal networks and data. Threat intelligence can surface various points in the process of insider actions both prior to and following data theft.

Information surfaced from sources across the open, deep, and dark web can prove useful. Threat research can monitor for leaks of sensitive information, surface valuable context to forecast potentially malicious activity, and surveil developing trends in how criminals are conducting the process of recruiting and using insiders. This kind of intelligence can also warn on direct threats to an organization.

Insider Threat Intelligence Monitoring

Monitoring for insider threats starts with the likely path of insiders maturation. Insider threat behaviors begin with naivety and mature to criminal collaboration and theft. Naive actors may violate rules due to ignorance. Self-interested individuals may recognize the policies but willfully violate them as they deem necessary as they're focused on job efficiency at the expense of security. This creates an extremely wide range of external indications to monitor, as insiders use the internet as frequently as the rest of society to comment, transact, purchase, and research.

Unfortunately, organizations often focus on monitoring either challenging or impossible to identify information, likely directly focused on their employees. Monitoring an employee's external behaviors is both disturbing and unproductive as an insider threat mitigation strategy. While public discontent, computer malfeasance, and suspicious working hours are possible behaviors associated with insider activity, these are not reliable indicators of the intent to betray. Many employees portray these behaviors at one point or another during their working life, and potential insiders may not exhibit any of these behaviors.

Threat intelligence surfaces relevant sources of information for analysts to rapidly identify potential insider activity. These indications alert the security analyst to research and, if necessary, escalate the incident for further investigation. Recorded Future can assist monitoring for insider threat indications in four areas:

1. Posted advertisements or solicitations on criminal forums and dark web
2. Proprietary information on sensitive sources
3. Proprietary assets or information on public code repositories
4. Employee PII or databases for sale

Criminal Advertisements and Solicitations

Industries **Banking, Finance**

Time ▾ Event Information

United Kingdom and ██████████ Banking Group PLC mentioned in Europe

JUL 24 2016 URGENT ██████████ BANK INSIDER REQUIRED IN THE UK
"URGENT ██████████ **BANK INSIDER REQUIRED IN THE UK**" [Cached](#)
Source AlphaBay Forum by stinkingrich on Jul 24, 2016, 05:01
<http://pwoah7foa6au2pul.onion/forum/index.php?threads/urgent-█████████-bank-insider-requ>

Mention

NOV 26 2016 i will pay \$120,000 for a bank insider.
"> pm me with what is needed possibly can get it done" [Cached](#)
Source AlphaBay Forum by Swipernoswipin on Nov 26, 2016, 19:41
<http://pwoah7foa6au2pul.onion/forum/index.php?threads/i-will-pay-120-000-for-a-bank-insider.113...> • Reference Actions • 1+ reference

Mention

NOV 26 2016 i will pay \$120,000 for a bank insider.
"i will pay \$120,000 for a bank insider." [Cached](#)
Source AlphaBay Forum by Swipernoswipin on Nov 26, 2016, 19:41
<http://pwoah7foa6au2pul.onion/forum/index.php?threads/i-will-pay-120-000-for-a-bank-insider.113...> • Reference Actions • 1+ reference

Seeking bank insiders on AlphaBay.

Title **Need Banking Malware - Inside Bank Job.: post #3**
Author **legitdealer**
Downloaded **Jan 31, 2017, 14:19**
Original URL <https://lampeduza.cm/topic/28135-need-banking-malware-inside-bank-job/#entry151049#5>

```
1. <html><body><div class="post entry-content " itemprop="commentText">
2. <!--cached-Fri, 27 Jan 2017 14:02:56 +0000--><p>My friend just told me that he has a inside in a
   bank ██████████ in usa and that the insider wanted to infect the bank with a malware now they don't
   really know anything about it that's why i made this post hoping someone with more experience
   would contact me and guide me true this job. Thanks</p>
3. <br/>
4. </div>
5. </body></html>
```

Insider looking to infect a bank with malware.

Bank and Experienced Spammer - Can mail millions a day. mentioned

JUL 1 2017

Experienced Spammer - Can mail millions a day.

"Have insider in bank if you can provide a good influx of logs then its jackpot" Forum Thread

Source AlphaBay Forum by cyberstalker, on Jul 1, 2017, 17:26

<http://pwoah7foa6au2pul.onion/forum/index.php?threads/experienced-spammer-can-mail-millions-a-d...> • Reference Actions • 1+ reference

Insider likely has lists of user details and is looking to spam or spearphish.

According to Avivah Litan, a Gartner analyst who specializes in information security, "Insiders are being actively recruited by criminals operating on the dark web, according to Gartner clients. Disgruntled employees working at companies across many sectors, such as financial services, pharma, retail, tech, and government are gladly selling their services to the bad guys in order to inflict harm on their employers. Seeking harm and revenge on employers is a bigger incentive for insider threats than is stealing money from employers, according to our clients."

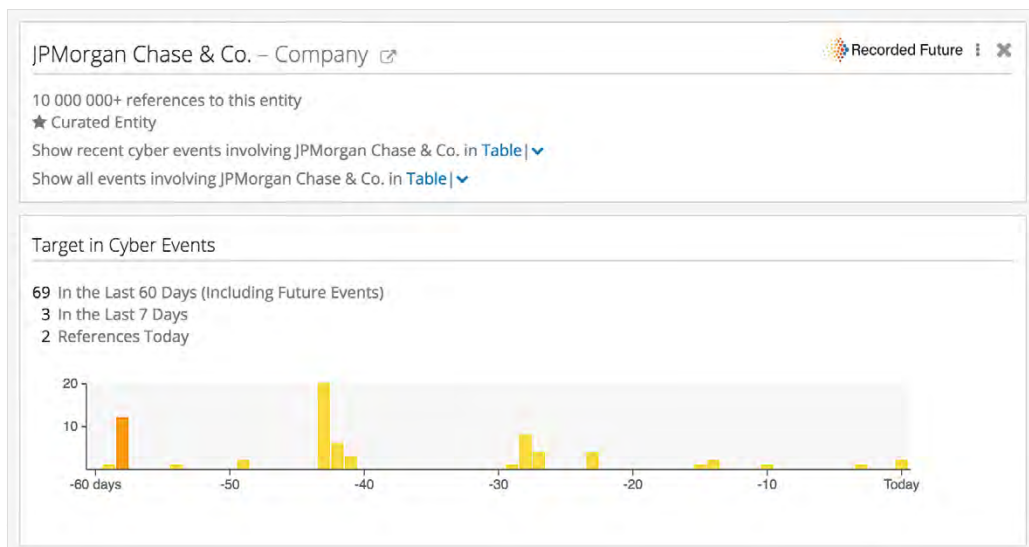
Criminal forums and marketplaces are well known for facilitating all types of illicit transactions. Insider threat advertisements are frequently used by actors promoting their illicit services on dark web sites, from retail cash-out services to carding operations, to bank insiders facilitating theft. Many of these advertisements lie on closed source forum sites, requiring extensive vetting and personas to maintain persistent access. Additionally, many services cannot regularly automatically harvest from closed sources or forums, so be sure to vet vendors carefully.

Insider threat alerting on closed forums or dark web takes three forms. **Monitoring for direct mentions of your organization or assets** are the first priority, as mentions likely indicate either targeting or a potential breach.

Industry mentions or tangential targeting are the next avenue of monitoring, as mentions of a "UK bank" or "#x of banking accounts" attempt to cover the source of information.

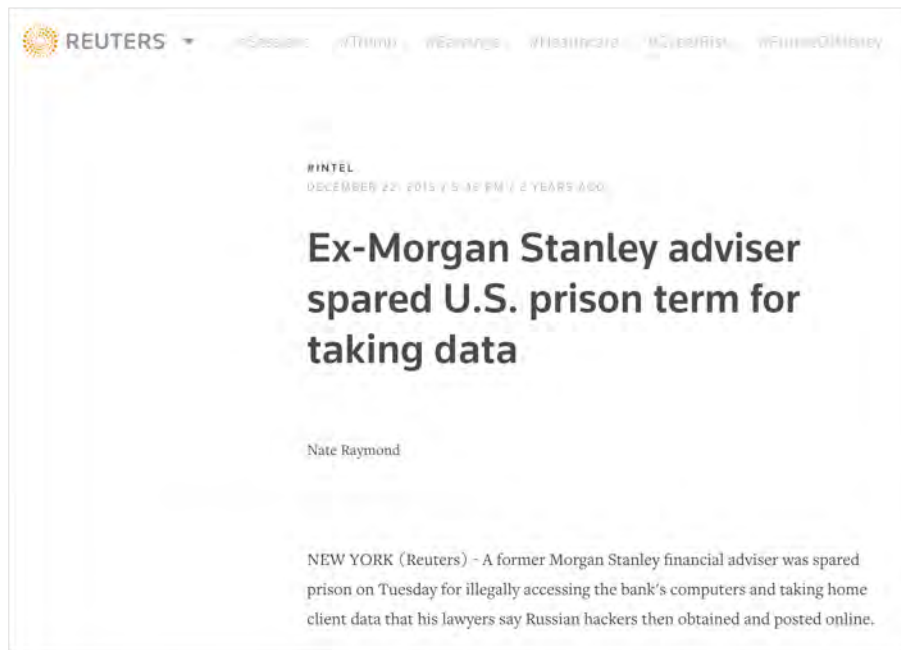
Finally, **presence on closed access forums** allows direct interaction with threat actors, possibly retrieving samples of allegedly stolen information and materials as validation. These interactions are difficult and private, but may prove exceptionally valuable.

Leaks of Betrayal

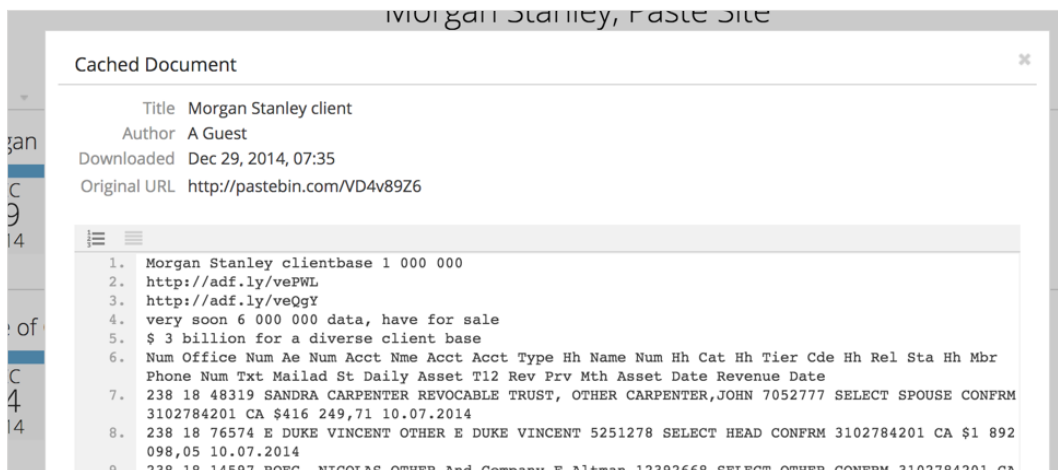


Brand and asset monitoring.

Monitoring for proprietary assets is a core use case for any threat intelligence tool. Open mentions of your information assets, brand names, and products in context should be continually monitored. Brand monitoring should also encompass BINs (Bank Identification Number) which will alert you to compromised card data. Assets may be mentioned for innocuous reasons, so it is important to identify the context where these mentions occur. Context may be an association with a particular event like a cyberattack or may be the venue where the asset is mentioned, such as a paste site or criminal forum. While this may not always target insider threats in particular, it allows your organization to quickly identify information posted which would immediately require investigation.



In late 2014, a 30-year-old employee at a financial services company [offered 6 million account records](#), including passwords and login data, for sale on Pastebin. Later, 1,200 accounts were actually spilled and offered as an enticement to purchase more accounts via Bitcoin. Overall, the financial firm determined the insider, Galen Marsh, accessed data on approximately 10% of the entire firm's wealth management clients.



Client account records uploaded to paste site.

Paste sites, criminal forums, and other sensitive sources tend to be volatile sources, with criminal actors posting and removing information rapidly. Strong threat intelligence tools may assist with caching these sources, further assisting any investigations into insider activity. Additionally, real-time alerting, breadth of coverage, and source selection should be taken into consideration when establishing monitoring on these sources.

Proprietary Code on Public Repositories

The screenshot displays a security tool interface titled "Code Repository, Finance". On the left, there is a sidebar with a list of filters: All Events, Author filters (96), Conversation (3), Corporate (71), Cyber (2), Indicators and Observables (39), List (10), Location (15), Organization (4), Person (104), Technology (2), and Other (4). The main area shows a list of events:

- Evaluate and Skandinaviska Enskilda Banken mentioned**
simulator-s390.h
AUG 1 2017
"EVALUATEISEB;" Cached
Source: GitHub by nodejs on Aug 1, 2017, 20:52
<https://github.com/nodejs/node/blob/988dab411523f83eca9b5311529f8288379e550f/deps/v8/src/s390/...> • Reference Actions • 1+ reference
- Germany and Deutsche Bank mentioned**
forbes_500_full.csv
JUL 31 2017
"441,Deutsche Bank,Germany,44.3,-1,9,1686,6,34,Financials,Major Banks,Europe" Cached
Source: GitHub by dharmk on Jul 31, 2017, 17:32
<https://github.com/dharmk/dharmk.github.io/blob/13e484d943cc41c7997024bde4894e14243a6c/forbes...> • Reference Actions • 1+ reference
- Business Transaction**
hosted_checkout.php
JUL 31 2017
"%{ MODULE_PAYMENT_PAYPAL_PRO_HS_GATEWAY_SERVER == 'Live' }%" Cached
Source: GitHub by brighthc on Jul 31, 2017, 04:07
https://github.com/brighthc/Puffisimo_Web/blob/7173c11307f688618889756950707db7d666596d/shop/ca... • Reference Actions • 1+ reference
- Telefonaktiebolaget LM Ericsson and UBS AG mentioned**
stratford_consulting_llc
JUL 29 2017
"UBS Group AG Buys 32,767 Shares of Ericsson" Cached
Source: GitHub by jeremy4555 on Jul 29, 2017, 14:06
<https://github.com/jeremy4555/courseEmbedding/blob/e4538e353f9915f49e1494a60c2d8804dce611f/com...> • Reference Actions • 1+ reference
- meminfo.bank mentioned**
mmu.c
JUL 29 2017
"*bank = &meminfo.bank{}" Cached

© Recorded Future

Proprietary code represents an immediate threat to a business's core infrastructure and operating applications. Many network and information technology workers utilize public source code for maintaining and improving company networks and applications. Additionally, they may contribute back to this open source code. While the contributions themselves are not necessarily cause for concern, the addition of company proprietary or sensitive information to open source code repositories certainly is.

In many cases, the proprietary code posted may be accidental, however this is still an insider posting sensitive information in a public forum where malicious actors can take advantage of the information. Monitoring for this information, and effective, timely remediation, improves the organization's security posture.



Conclusions

Insider threat is a complex problem requiring fusion of security teams, business operational teams, and technology to adequately address. Current strategies to mitigate the risks from insiders tend to focus solely on activity inside the network, but behaviors are easily misjudged and the risk from noisy alerts is high. Where the insider must expose themselves is in finding a method to make effective use of their privileged access or exfiltrated data. External threat intelligence can provide valuable monitoring, investigative, and contextual reporting in real time, while requiring few resources to maintain. As many as [6-in-10 financial organizations are yet to subscribe to third-party threat intelligence](#), and the same number agree that intelligence sharing on security threats within the financial services industry must improve. As security loopholes continue to close, criminal actors will continue to identify exploitable opportunities using available resources. Likewise, nation-state actors will utilize insiders for persistent access to hard targets.

About Recorded Future

Recorded Future delivers threat intelligence powered by machine learning, arming you to significantly lower risk. We enable you to connect the dots to rapidly reveal unknown threats before they impact your business, and empower you to respond to security alerts 10 times faster. Our patented technology automatically collects and analyzes intelligence from technical, open, and dark web sources to deliver radically more context than ever before, updates in real time so intelligence stays relevant, and packages information ready for human analysis or instant integration with your existing security systems.

Recorded Future, 363 Highland Avenue, Somerville, MA 02144 USA | © Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners. | 08/17