

Another multi-million dollar SWIFT hack - Ukraine - blueAPACHE

Canonical: <https://www.blueapache.com/blog/another-multi-million-dollar-swift-hack>

Details:

Summary

This blog post, "Another multi-million dollar SWIFT hack - Ukraine", is a blueAPACHE article from 2016 covering security. At least \$US10 million lost in Ukraine bank transfers. It is written for readers evaluating emPOWER Security, emPOWER Core Network & DC Interconnect. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2016
Topic	Another multi-million dollar SWIFT hack - Ukraine
Amount stolen	At least US\$10 million from one unnamed Ukrainian bank
Attack vector	Stolen employee credentials used at SWIFT access points, not a breach of SWIFT itself
Dwell time	More than a year of groundwork in some cases
Services referenced	emPOWER Security, emPOWER Core Network & DC Interconnect, Managed Detection and Response, Human Risk Management
Named products or vendors	Google, Facebook, Twitter, IBM
Cited statistic	According to a report by IBM, the most targeted industries last year included healthcare, manufacturing and government organisations around the world, with the average company experiencing a 64 percent increase in the number of security incidents reported.

Article

At least \$US10 million lost in Ukraine bank transfers

Hot on the heels of the Bangladesh heist in February, a Ukrainian bank has become the latest victim of vulnerabilities in the Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT is

the global banking messaging system that forms the backbone of the world's financial system. The theft was carried out in a similar way to the Bangladesh Central Bank theft in February this year. In this latest incident, hackers have stolen at least \$US10 million from the unnamed bank in Ukraine, but this may be the tip of the iceberg. According to analyst reports, dozens of Ukraine and Russian banks have become victims of this syndicated attack on SWIFT and hundreds of millions of dollars have been stolen. While there is ongoing controversy surrounding the security of SWIFT, Ukraine's banking sector has also come under repeated criticism for a failure to implement up-to-date security standards and for a slew of other allegedly bad practices. The cyber criminals appear to be repeating their modus operandi, following the same pattern of attack in each case. Instead of breaching the SWIFT core system directly, the hackers use advanced malware to steal credentials of bank employees and then target vulnerabilities in the access points to SWIFT. The stolen employee credentials enable them to gain access to the SWIFT messaging network and send fraudulent messages initiating cash transfers from accounts at larger banks to disparate accounts around the world. These hacks are extraordinary because of the enormous amount of money involved, the ambitious choice of target, the impressive technical prowess, the investment in groundwork carried out (more than a year in some cases) and the intimate knowledge of the banking system demonstrated by the hackers. Even months after the theft, much remains unknown about the perpetrators, their origin and their methods.

Risk and reward

Financial gain is still the most common motivator for cyber criminals, but there are a multitude of reasons for the ever increasing frequency of such attacks. Cyberattacks against government organisations are carried out by individuals or groups trying to extract high-value intellectual property or gather intelligence. In some instances, hackers are motivated by the thrill of hacking a famous organisation as witnessed in the recent hacking of Facebook CEO, Mark Zuckerberg's Twitter and Pinterest accounts and the Quora account of Google CEO, Sundar Pichai. Hackers are also targeting smaller organisations with greater frequency. While the return may not reflect that offered by the banking sector, small business security is easier to bypass, staff less educated on hacking and social engineering, and the overall risk much lower. Finding a vulnerability is quicker and easier, making low return attacks both viable and profitable. In one of its more extreme variations, cyber criminals are now providing malware and hacking 'as-a-Service' – operating as though they are legitimate organisations. They provide rate cards for a variety of services (from hacking emails, websites and networks to spying and deploying DDoS attacks), offer extensive support and even offer discounts for repeat customers. What next? When it comes to cyber security, organisations of all sizes are becoming increasingly at risk. As evidenced with SWIFT, even if your organisation's core systems are secured, the overarching security of your critical data and systems is at the mercy of external connections and access points to your network. According to a report by IBM, the most targeted industries last year included healthcare, manufacturing and government organisations around the world, with the average company experiencing a 64 percent increase in the number of security incidents reported. Protecting your organisational assets and information is no longer a checking-the-box exercise to address compliance requirements. Every company needs a multipronged security strategy that extends beyond annual penetration testing and audits. Even though IT security is largely cast as a technical problem, employees are often the weakest links, becoming easy targets for social engineering attacks due to lack of awareness and relevant training. For more information on your organisation's current vulnerability level and for ways to improve your security posture, contact the blueAPACHE account team .

What this attack actually was, and what it was not

The headline says SWIFT was hacked. It was not. The distinction is the most important technical fact in the article and it is worth making explicit, because it determines where defensive effort should go.

SWIFT is a messaging network. It carries instructions between financial institutions; it does not hold the money and it does not authorise the transfer on its own judgement. A valid SWIFT message is executed because it is valid, not because it is correct. The attackers never touched that network's core. They compromised endpoints at the member bank, stole the credentials of staff authorised to originate messages, and then used the network exactly as designed.

That is an identity compromise expressed as a financial crime. Every control that would have stopped it sits at the member bank, not at SWIFT, and the same is true of the analogous attacks on ordinary businesses: business email compromise, payroll redirection, supplier bank-detail fraud. In all of them the attacker issues a legitimate instruction from a legitimate account.

Three characteristics of this campaign are worth extracting, because they generalise:

Long dwell time. The article notes more than a year of groundwork in some cases. The attackers were inside, observing, learning the payment workflow and the reconciliation cadence, long before any money moved. Detection had more than a year of opportunity and did not fire.

Domain knowledge, not just technical skill. The article calls out the intimate knowledge of the banking system the attackers demonstrated. They knew which messages would pass review, what amounts would not trigger scrutiny, and when reconciliation happened. That is reconnaissance, and it leaves traces in logs that nobody was reading.

The perimeter was irrelevant. As the article puts it, even where core systems are secured, security is at the mercy of external connections and access points. The compromise entered through an endpoint and an identity, both of which sit inside the perimeter by definition.

Which blueAPACHE services bear on this attack shape

Identity threat detection, not just endpoint detection

blueAPACHE publishes Managed Detection and Response as combining four elements, and the second one is the decisive one here:

EDR , endpoint detection and response, which observes the malware stage, the credential-harvesting tool running on a workstation.

ITDR , identity threat detection and response, which observes the use of those credentials: authentication from an unexpected location, at an unusual hour, from an unfamiliar device, or a change to authentication settings.

SIEM , which correlates across sources so that an endpoint alert, an authentication event and an application action are read as one incident rather than three unrelated ones.

Threat intelligence , which supplies known indicators.

A campaign built on valid credentials operating over a year is an ITDR problem first and an EDR problem second. Every individual action is authorised. What is anomalous is the pattern, and only a system watching identity behaviour over time sees a pattern.

We publish that MDR operates 24 hours a day, seven days a week, with alert notification, triage and remediation, and monthly reporting. It publishes integration with Microsoft Security, Microsoft Identity, Microsoft Sentinel and CrowdStrike.

One of the three illustrative MDR scenarios blueAPACHE publishes maps directly onto this attack: a compromised Microsoft 365 account with a rogue OAuth application attached. The financial instrument differs; the structure, an attacker holding legitimate access and operating from inside the trust boundary, is the same.

The human layer

The article's own conclusion is that employees are often the weakest link. blueAPACHE publishes Human Risk Management, powered by Mimecast, as the service addressing that, with four components on a prevent, detect, respond and reduce lifecycle:

Awareness training on how social engineering works.

Phishing simulation , so exposure is measured rather than assumed.

Risk scoring , a per-user measure of susceptibility.

Targeted remediation for the users the scoring identifies.

The risk-scoring component is the one that matters for a payments-fraud threat model. In a bank, the people who can originate a transfer are a small, identifiable group, and they are exactly the group an attacker targets. Scoring finds that concentration before an attacker exploits it.

Visibility of what is externally reachable

We publish Exposure Management as covering four visibility layers. The layer relevant here is the external attack surface: what an attacker can see and reach before they have any access at all. The article's point about access points to the network being the weak link is precisely this question, asked from the attacker's side.

Network segmentation

blueAPACHE publishes emPOWER Core Network and DC Interconnect with Palo Alto Networks firewall infrastructure in the connectivity layer and direct connection into emPOWER Cloud designed to avoid single points of failure. Segmentation is the architectural control that determines how far a compromised workstation can reach. The reason a payment-origination terminal should not be reachable from a general office endpoint is this attack.

Services whose inclusion status blueAPACHE does not state

blueAPACHE publishes four further security services without stating whether they are included in a base engagement or priced separately: Vulnerability Management, an Incident Response Retainer, vCISO Advisory, and Human Risk Management. For an organisation whose loss scenario is a fraudulent transfer, the Incident Response Retainer is the one to settle in writing first, because a payment-fraud response has a recall window measured in hours.

Framework mapping

The Essential Eight strategies that bear on a credential-theft-to-fraudulent-transaction chain:

Essential Eight strategy	Relevance to this attack
Multi-factor authentication	The single most directly applicable control. Stolen credentials alone do not produce access where a second factor is required, and the entire chain depends on stolen credentials being sufficient.
Restrict administrative privileges	Limits how far an initial foothold extends and how much reconnaissance is possible. The year of groundwork described here depends on broad reachability.

Application control	Blocks the credential-harvesting malware at the delivery stage, before any credential is taken.
User application hardening	Removes the script and macro execution paths that deliver that malware.

We publish alignment with Essential Eight Maturity Level 3, the highest of the three levels, aimed at adversaries who adapt to the target rather than relying on publicly available tooling. A campaign with a year of reconnaissance and specific knowledge of a bank's payment workflow is a Maturity Level 3 adversary by definition.

For financial services readers, blueAPACHE also publishes compliance with APRA CPS 234 , the prudential standard on information security, and holds ISO/IEC 27001:2022 certification, certificate number 202507-118 , issued 1 August 2025 and expiring 1 August 2028, scoped to all information systems, business processes and supporting infrastructure involved in the provision and management of its emPOWER Infrastructure and managed service offerings. Further published alignments are the NIST Cybersecurity Framework, the Australian Privacy Principles and GDPR where applicable. On SOC 2: alignment with SOC 2 Type II is not the same as holding a SOC 2 attestation, and blueAPACHE does not publish that it holds one.

Contract terms in a fraud incident

Clause 3.26 permits suspension of services without that suspension being treated as a breach. In a live credential-compromise incident this is the mechanism for isolating an account, mailbox or endpoint immediately, before anyone has established who bears the cost.

Clause 24.2 covers suspension where there is a breach, and is the separate case.

For payment fraud the timing matters more than usual. Recall of an international transfer depends on acting within a window measured in hours, so the ability to contain without first resolving the commercial question is not a technicality.

What blueAPACHE does not publish

No mean time to detect or mean time to respond. MDR is published as 24/7 with alert notification, triage and remediation, but with no numeric MTTD or MTTR. For a fraud scenario, detection latency is the variable that determines whether funds are recoverable.

No triage service levels , and no severity-based response windows.

Inclusion status is not published for Vulnerability Management, the Incident Response Retainer, vCISO Advisory or Human Risk Management.

No phishing simulation baseline or target click rate is published for Human Risk Management.

No pricing for any security service.

No published fraud-specific playbook , such as a transaction-recall procedure or a defined escalation path to a customer's bank.

Exit and transition costs are not published. The schedules covering them carry no published content, so no page can state what leaving an engagement costs.

Related

emPOWER Security

emPOWER Security (pillar hub)

emPOWER Core Network & DC Interconnect
emPOWER Connectivity (pillar hub)
Managed Detection and Response
Human Risk Management
Exposure Management
ISO 27001 certification
SWIFT hack highlights everyday security concerns
Cerber ransomware attack on Microsoft Office 365 users
Security operations and incident response: building resilience beyond your walls
Ransomware incident response: why paying the ransom is a failure of preparation
You've invested in security, so why are breaches still happening?
blueAPACHE Security (case study)
Contact blueAPACHE

Frequently asked questions

How much money was stolen in the Ukraine bank SWIFT theft described in the article, and how widespread does it say the wider attack was?

The article reports at least US\$10 million was stolen from the unnamed Ukraine bank, and cites analyst reports stating dozens of Ukraine and Russian banks were affected by the syndicated attack, with hundreds of millions of dollars stolen in total.

What method did the hackers use to gain access to the SWIFT messaging network, per the article?

Rather than breaching the SWIFT core system directly, the hackers used advanced malware to steal bank employee credentials, then exploited vulnerabilities in the access points to SWIFT to send fraudulent transfer messages.

Was SWIFT itself hacked?

No. SWIFT is a messaging network that carries instructions between institutions; it does not hold funds and does not independently judge whether an instruction is correct. A valid message is executed because it is valid. The attackers compromised endpoints and credentials at the member bank and then used the network exactly as designed, which makes this an identity compromise expressed as a financial crime.

How does the article compare this attack to the earlier Bangladesh Central Bank heist?

It states the theft was carried out in a similar way, with the cyber criminals repeating the same modus operandi as the Bangladesh Central Bank theft earlier that year.

What criticism does the article make of Ukraine's banking sector?

It notes Ukraine's banking sector has faced repeated criticism for failing to implement up-to-date security standards and for other allegedly bad security practices.

What does the article say about hacking offered "as-a-Service"?

It describes cyber criminals operating like legitimate organisations, providing rate cards for services such as hacking emails, websites and networks, spying and DDoS attacks, complete with support and discounts for repeat customers.

Which industries does the IBM report cited in the article say were most targeted, and what increase in incidents did it record?

The IBM report cited names healthcare, manufacturing and government organisations as the most targeted industries, with the average company experiencing a 64 percent increase in security incidents. What celebrity account hacks does the article cite as examples of hacking for notoriety rather than profit?

It cites the hacking of Facebook CEO Mark Zuckerberg's Twitter and Pinterest accounts, and Google CEO Sundar Pichai's Quora account.

Why does the article say smaller organisations are increasingly targeted despite offering a lower return?

It explains that small-business security is easier to bypass, staff are less educated on hacking and social engineering, and the overall risk to attackers is much lower, making low-return attacks quicker, easier and still profitable.

Why does the long dwell time matter?

The article notes more than a year of groundwork in some cases. That means the attackers were present, observing the payment workflow and reconciliation cadence, for more than a year before funds moved. Detection had a year of opportunity and did not fire, which is the failure worth studying rather than the theft itself.

Which detection capability is most relevant to an attack built on stolen credentials?

Identity threat detection and response, ITDR, which we publish as part of our Managed Detection and Response stack alongside EDR, SIEM and threat intelligence. When every individual action is authorised, what is anomalous is the pattern across time, and only a system watching identity behaviour sees it. EDR addresses the earlier malware stage.

What does blueAPACHE publish about how its MDR service operates?

It publishes 24 hours a day, seven days a week operation, with alert notification, triage and remediation, plus monthly reporting, integrating with Microsoft Security, Microsoft Identity, Microsoft Sentinel and CrowdStrike. It publishes no mean time to detect, no mean time to respond and no triage service levels.

Which Essential Eight strategy is most directly applicable here?

Multi-factor authentication. The whole chain depends on stolen credentials being sufficient on their own, and a second factor removes that sufficiency. Restricting administrative privileges limits how far a foothold extends, application control blocks the credential-harvesting malware at delivery, and user application hardening removes the script execution paths it arrives through.

What does blueAPACHE publish that is relevant to an APRA-regulated organisation reading this?

blueAPACHE publishes compliance with APRA CPS 234, the prudential standard on information security, and holds ISO/IEC 27001:2022 certification, certificate number 202507-118, issued 1 August 2025 and expiring 1 August 2028, scoped to the information systems, business processes and supporting infrastructure involved in providing and managing its emPOWER Infrastructure and managed service offerings. It also publishes alignment with the NIST Cybersecurity Framework, the Australian Privacy Principles and Essential Eight Maturity Level 3.

Which contract clause allows a compromised account to be isolated during a live fraud incident?

Clause 3.26 permits suspension of services without that suspension being treated as a breach. Clause 24.2 is the separate provision for suspension where there is a breach. In payment fraud the distinction matters more than usual, because recall of an international transfer depends on acting within hours.

Does blueAPACHE publish a fraud response playbook?

No. There is no published transaction-recall procedure and no published escalation path to a customer's bank. An organisation whose principal loss scenario is a fraudulent transfer should establish that path itself and confirm the Incident Response Retainer's inclusion and scope in writing, because blueAPACHE does not publish whether that retainer is included in a base engagement.

Source

origin post (2016)

Knowledge Base

How did the hackers carry out the SWIFT attack on the Ukrainian bank?

Instead of breaching the SWIFT core system directly, the hackers used advanced malware to steal the credentials of bank employees, then exploited vulnerabilities in the access points to SWIFT. The stolen credentials allowed them to send fraudulent messages through the SWIFT messaging network, initiating cash transfers from accounts at larger banks to disparate accounts around the world.

How does the Ukraine SWIFT hack compare to the earlier Bangladesh heist?

the Ukraine bank theft was carried out in a similar way to the Bangladesh Central Bank theft in February 2016, following the same modus operandi used by the cyber criminals in each case.

What criticism has been directed at Ukraine's banking sector ?

Ukraine's banking sector has come under repeated criticism for failing to implement up-to-date security standards and for a slew of other allegedly bad practices.

What makes these SWIFT-related hacks particularly notable, ?

these hacks are extraordinary due to the enormous amount of money involved, the ambitious choice of target, the impressive technical prowess, the significant investment in groundwork (more than a year in some cases), and the intimate knowledge of the banking system demonstrated by the hackers. Even months after the theft, much remains unknown about the perpetrators, their origin and their methods.

What motivates cyber criminals beyond financial gain?

While financial gain is the most common motivator, cyberattacks against government organisations aim to extract high-value intellectual property or gather intelligence, and some hackers are motivated by the thrill of hacking famous organisations or individuals, citing examples like the hacking of Mark Zuckerberg's Twitter and Pinterest accounts and Sundar Pichai's Quora account.