Threats from the Dark Side – A Dark Web Tour from a PCI DSS Perspective

Christopher Strand, Chief Risk and Compliance Officer
Cybersixgill

PCI Security Standards Council®

cybersixgill

Agenda

A Dark Web Tour from a PCI DSS perspective

How threat intelligence is used against you: techniques and tactics used on the dark web to exploit critical and sensitive data.

How payment data and systems are targeted, used, and sold by the criminal underground.

How PCI DSS v4.0 helps to counter the problem in the dark web environment to prevent threat actors from exploiting systems and data.

The Attack Trend Has Been Changing

14+ Billion

Global Data Records
Lost Since 2013

40.4+ Billion

Global Data Records
Exposed in 2021

Source: Tenable's 2021 Threat Landscape Retrospective (TLR) report

Signal to Noise Ratio of Data Protection

The Levels of Dark Web Cyber Intelligence

Bad actors use cyber threat intelligence (CTI) to create opportunities throughout cyberspace. Accessing various underground sources for continually assembling attacks and hiding their tracks

Clear Web

Paste sites (e.g. pastebin), Reddit, 8chan, NVD, Twitter (secondary+direct), GitHub (Secondary+direct)

Deep Web

Open and closed (invite-only) forums, markets, credit card markets, paste sites and IRC channels

Dark Web

Open and closed (invite-only) forums, markets, credit card markets, paste sites and IRC channels, Dread, Zeronet

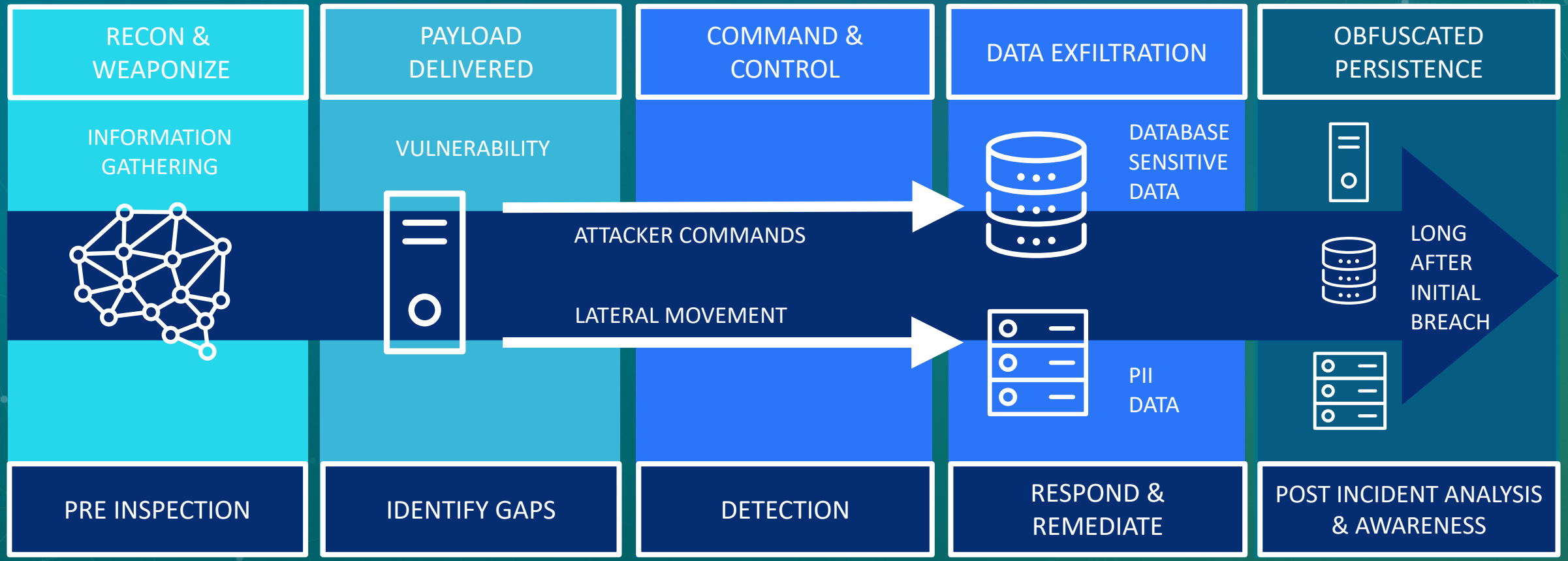
Social Messaging

Open and closed (invite-only) groups and channels on **Telegram, Discord** and **QQ**, **ICQ**

In a Dark Web Minute

Organizations today swim in data. We performed an exercise to feel the ‘Pulse of the Underground’ - what happens in the deep and dark web in a minute. The results were staggering.

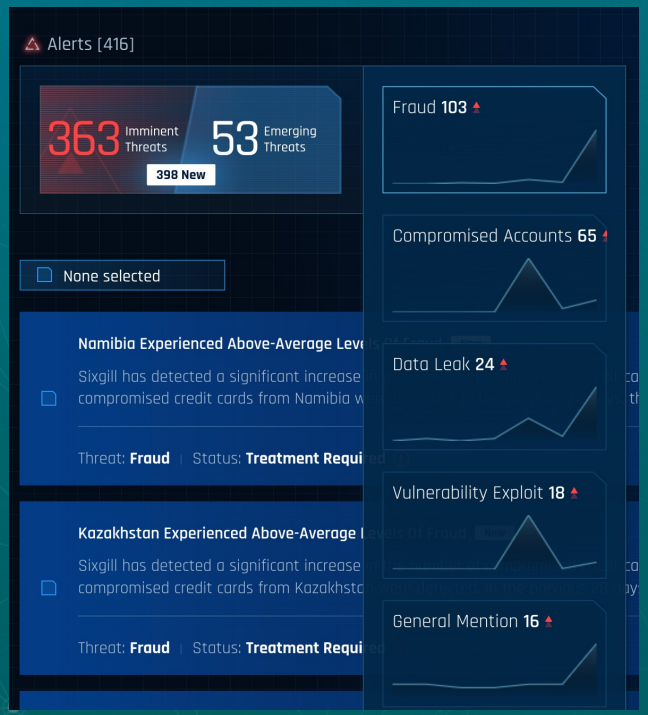
Attackers utilize preemptive and proactive techniques for exploits

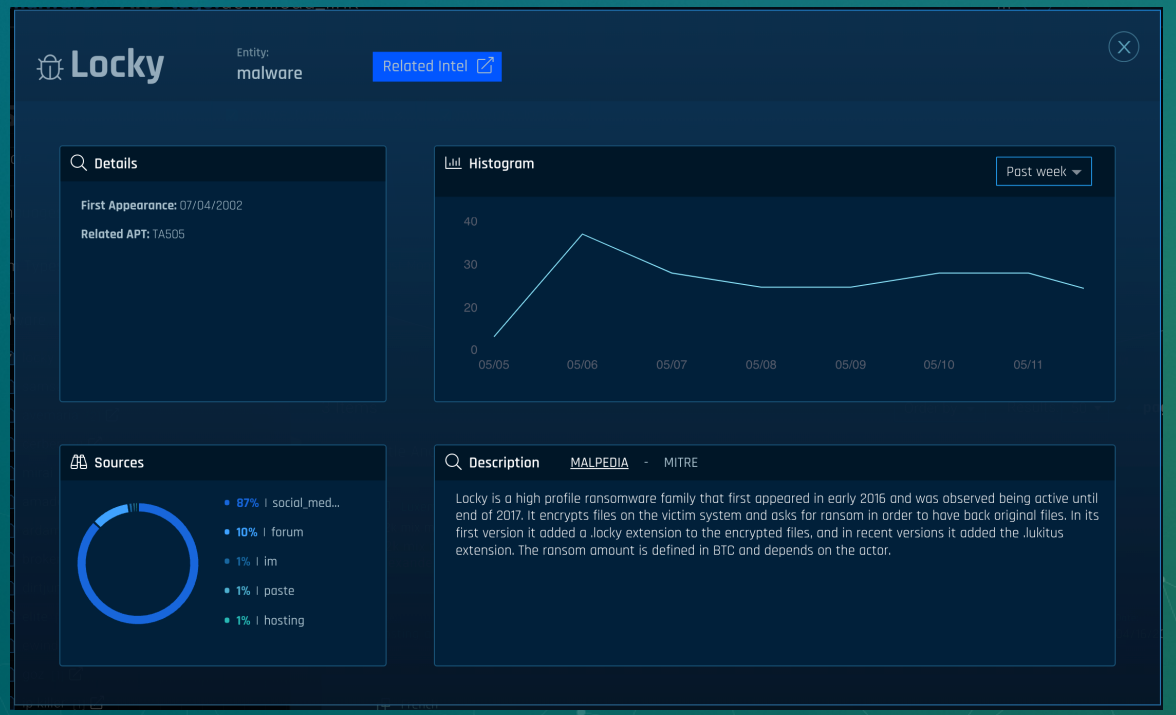


PRE AND POST SECURITY CONTROLS RESPONSIBLE FOR PREVENTING AN EXPLOIT

Financial Sector System Targeting Escalates with Market Changes

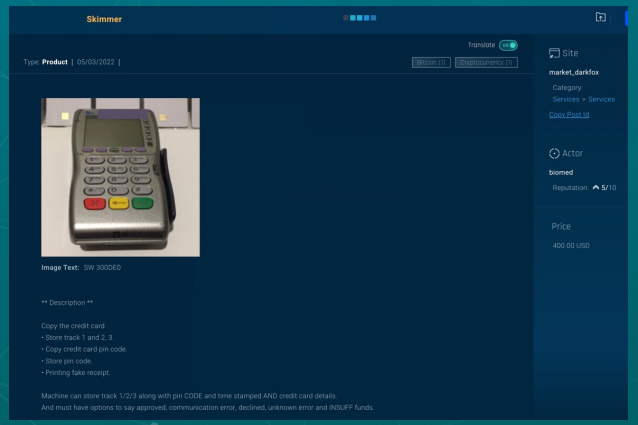
Dark Web examples showing escalation of financial and payment system related targeting

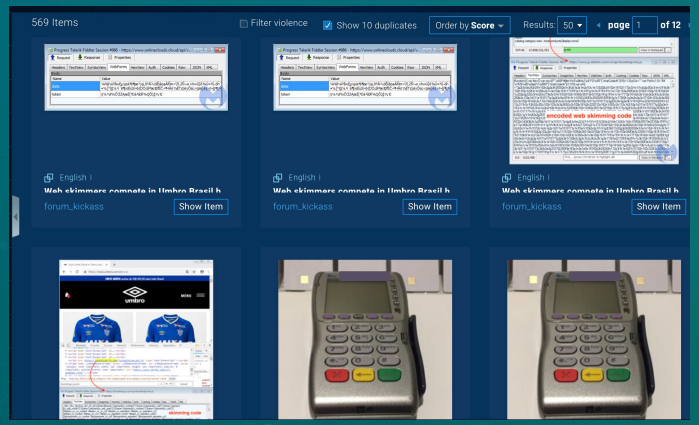


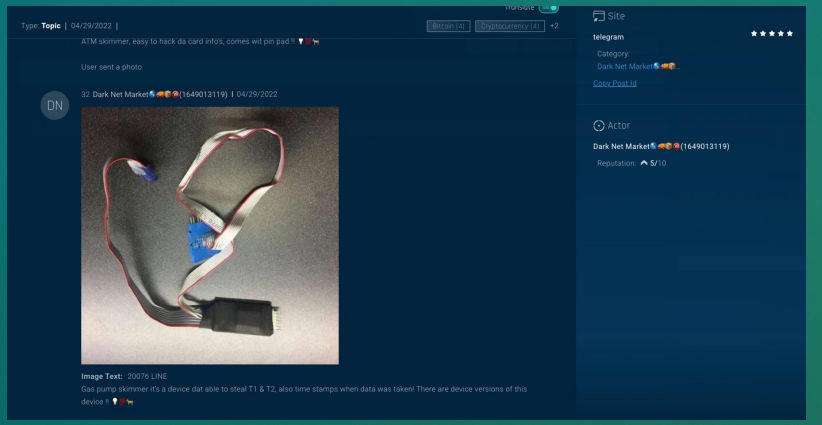


Payment Related Data with Personal Information in Scope and Value Continues to Grow

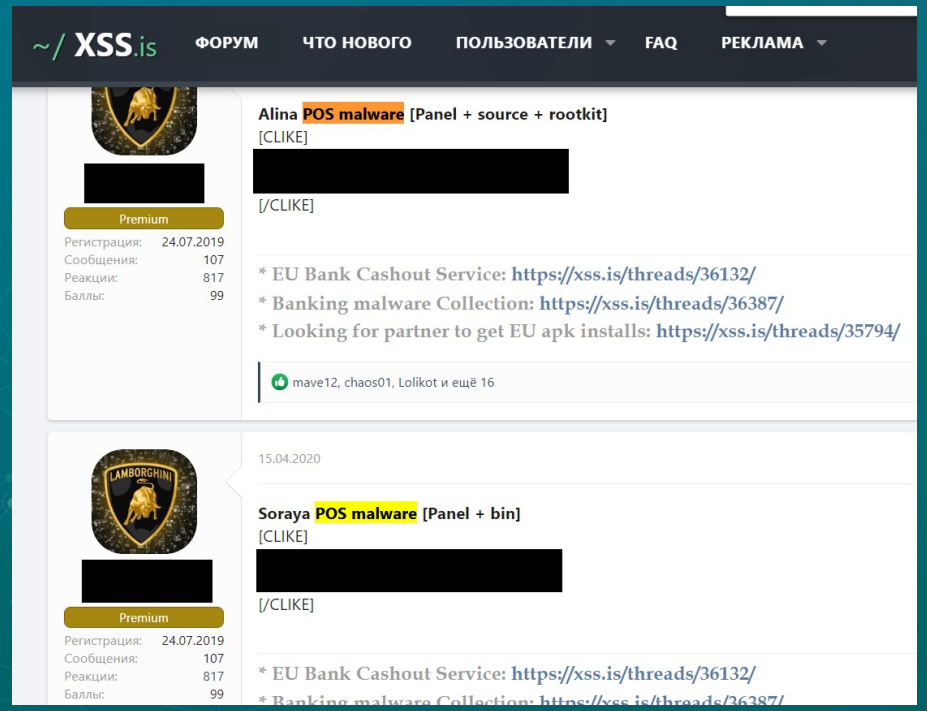
Dark Web examples showing targeting financial data via system security gaps

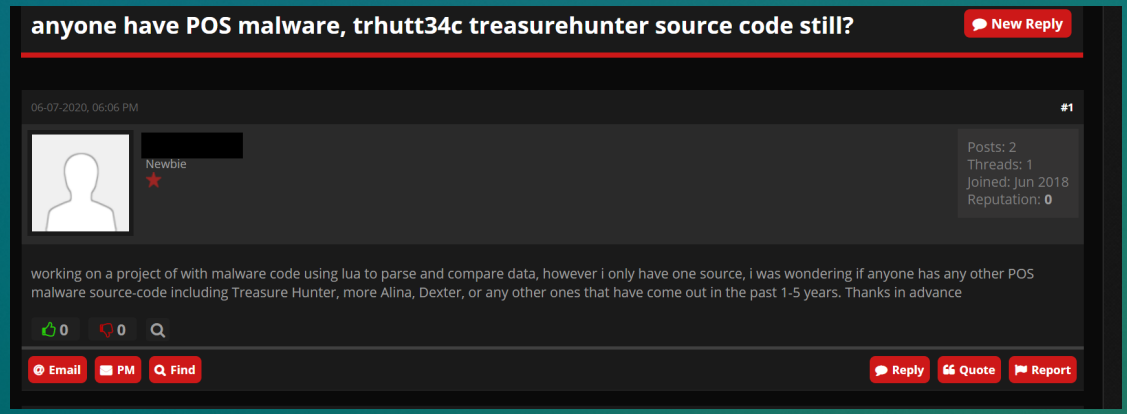






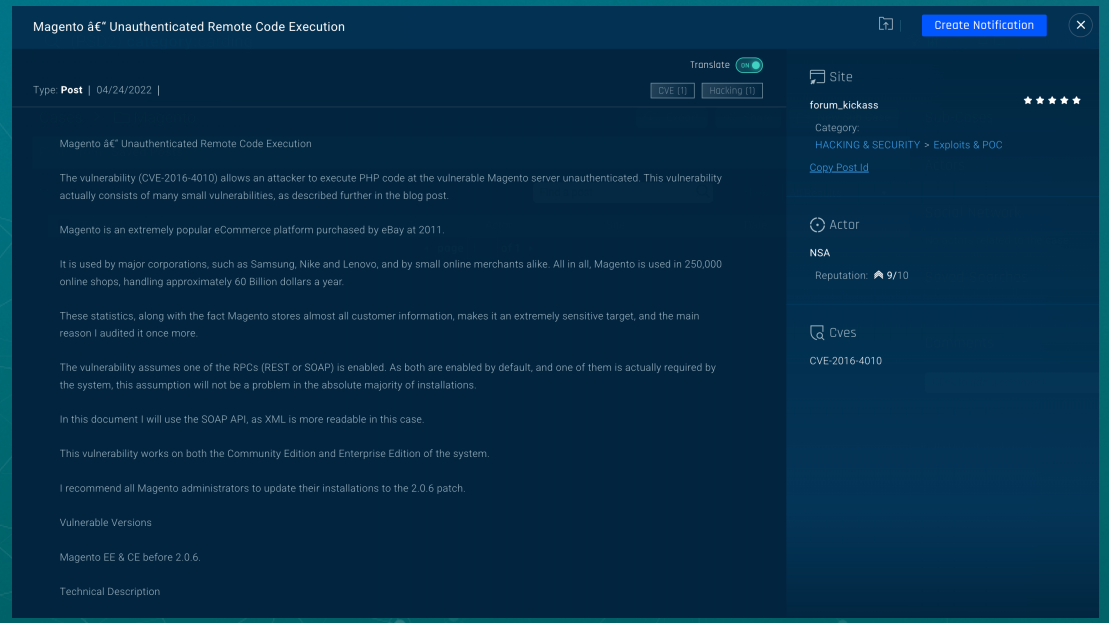
Dark Web Forum Payment System Targeting

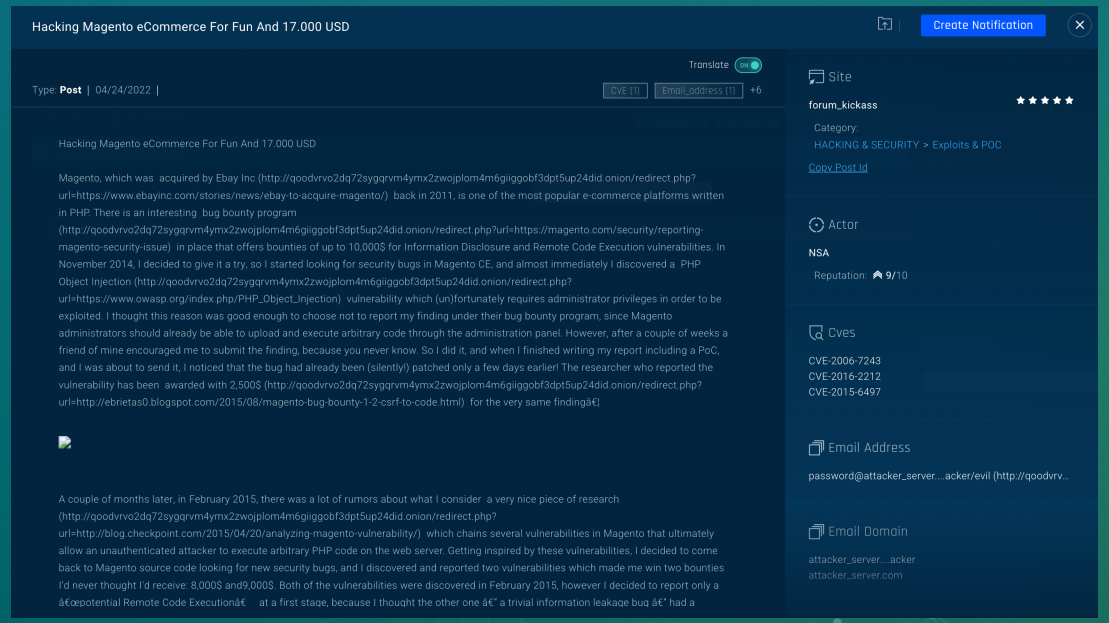




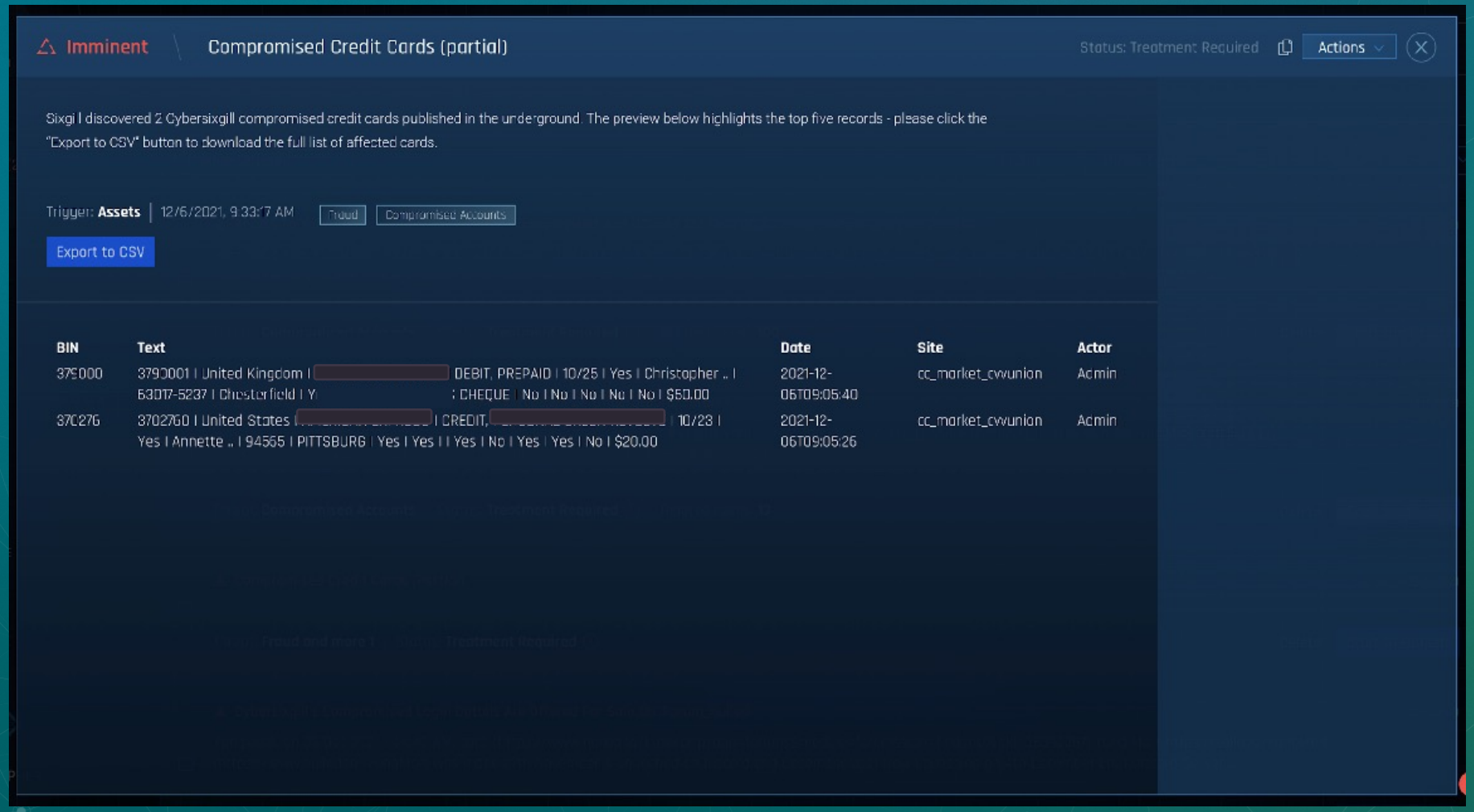
Payment Systems in the Cross-hairs

Dark Web examples showing targeting payment system data via system security gaps





Find and Protect ALL Payment Related Data



How the PCI DSS v4.0 Helps to Counter Growing Attacks from the Dark Web

Vulnerability and Gap Prioritization

PCI DSS v4.0 Requirement 6.3:

- Can help to uncover outlying gaps and vulnerabilities that attackers are capitalizing on and exploiting
- Will help to continually measure the real risk of any vulnerabilities across your enterprise
- Will ensure that the right priority is applied to the right vulnerabilities with measurable enforcement

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	**6.3.1.a** Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement. **6.3.1.b** Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. **Good Practice** Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution. An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*
Customized Approach Objective		
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
Applicability Notes		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideral potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-ris critical to the environment. • Vulnerabilities for bespoke and custom, a third-party software (for example operatir systems and databases) are covered.	**6.3.1.a** Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement. **6.3.1.b** Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and	Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. **Good Practice** Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an zation's environment and risk-assessment gy. an entity is assigning its risk rankings, it consider using a formal, objective, ble methodology that accurately portrays ks of the vulnerabilities pertinent to the zation and translates to an appropriate entity-assigned priority for resolution. An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*
Customized Approach Objective		
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
Applicability Notes		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

industry-recognized sources for security vulnerability information

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	**6.3.1.a** Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement. **6.3.1.b** Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. **Good Practice** Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution. An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*
Customized Approach Objective		
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
Applicability Notes		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements **6.3.1** Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. **Customized Approach Objective** New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed. **Applicability Notes** This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.	**Defined Approach Testing Procedures** **6.3.1.a** Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement. **6.3.1.b** Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and	**Purpose** Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. **Good Practice** Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an rganization's environment and risk-assessment trategy. hen an entity is assigning its risk rankings, it hould consider using a formal, objective, stifiable methodology that accurately portrays e risks of the vulnerabilities pertinent to the rganization and translates to an appropriate ntity-assigned priority for resolution. n organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*

vulnerabilities considered to be a high-risk or critical to the environment

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	**6.3.1.a** Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement. **6.3.1.b** Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. **Good Practice** Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution. An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*
Customized Approach Objective		
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
Applicability Notes		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and cor potential impact. • Risk rankings identify, at a minimu vulnerabilities considered to be a l critical to the environment. • Vulnerabilities for bespoke and cu third-party software (for example c systems and databases) are cove	**6.3.1.a** Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement. **6.3.1.b** Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and	Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. **Good Practice** Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an s environment and risk-assessment ty is assigning its risk rankings, it der using a formal, objective, thodology that accurately portrays e vulnerabilities pertinent to the and translates to an appropriate ed priority for resolution. on's processes for managing s should be integrated with other processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*
Customized Approach Objectiv New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
Applicability Notes This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	**6.3.1.a** Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement. **6.3.1.b** Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. **Good Practice** Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution. An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*
Customized Approach Objective		
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
Applicability Notes		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimu vulnerabilities considered to be a l critical to the environment. • Vulnerabilities for bespoke and cu third-party software (for example c systems and databases) are cove	**6.3.1.a** Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement. **6.3.1.b** Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. **Good Practice** Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. ty is assigning its risk rankings, it der using a formal, objective, thodology that accurately portrays e vulnerabilities pertinent to the and translates to an appropriate ed priority for resolution. on's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*
Customized Approach Objective New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
Applicability Notes This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

This requirement is not achieved by, nor is it the same as, vulnerability scans

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements **6.3.1** Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. **Customized Approach Objective** New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed. **Applicability Notes** This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.	**Defined Approach Testing Procedures** **6.3.1.a** Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement. **6.3.1.b** Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	**Purpose** Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. **Good Practice** Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution. An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*

for a process to actively monitor industry sources

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	**6.3.1.a** Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement. **6.3.1.b** Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. **Good Practice** Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution. An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*
Customized Approach Objective		
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
Applicability Notes		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk critical to the environment. • Vulnerabilities for bespoke and custom, an third-party software (for example operating systems and databases) are covered.	**6.3.1.a** Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement. **6.3.1.b** Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. **Good Practice** Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. tity is assigning its risk rankings, it ider using a formal, objective, ethodology that accurately portrays he vulnerabilities pertinent to the and translates to an appropriate ed priority for resolution. tion's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*
Customized Approach Objective New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
Applicability Notes This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

Processes should support ongoing evaluation of vulnerabilities

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	**6.3.1.a** Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement. **6.3.1.b** Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. **Good Practice** Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution. An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE. *(continued on next page)*
Customized Approach Objective		
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
Applicability Notes		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

6.3 In Practice Combined with Dark Web Intelligence to Find Outliers

6.3 In Practice Combined with Dark Web Intelligence to Find Outliers

CVE-2020-0989	5.14	2.1	5.5
CVE-2020-16999	5.11	2.1	5.5
CVE-2020-10002	5.09	2.1	5.5
CVE-2020-4842	5.04	4	4.9
CVE-2019-1440	5.01	2.1	

An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1436.

CVE-2019-1440

An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1436.

CVE Score Card

Dynamic Vulnerability Exploit Score

Current Score	**0**
Highest Score	**5.01**
Previously Exploited	**2.5**

CVSS 3.1

Score	N/A
Published	**11/12/2019**
Modified	**11/13/2019**

CVSS 2.0

Score	**2.1**
Published	**11/12/2019**
Modified	**11/13/2019**

Vulnerability Prioritization Using Dark Web Intelligence (Windows EOL)

CVE-2017-0147

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted packets, aka "Windows SMB Information Disclosure Vulnerability."

CVE Score Card

Dynamic Vulnerability Exploit Score	
Current Score	9.97
Highest Score	10
Previously Exploited	10

CVSS 3.1	
Score	5.9
Published	03/16/2017
Modified	06/20/2018

CVSS 2.0	
Score	4.3
Published	03/16/2017
Modified	06/20/2018

Activity by Date

Date: Past year

846 Items

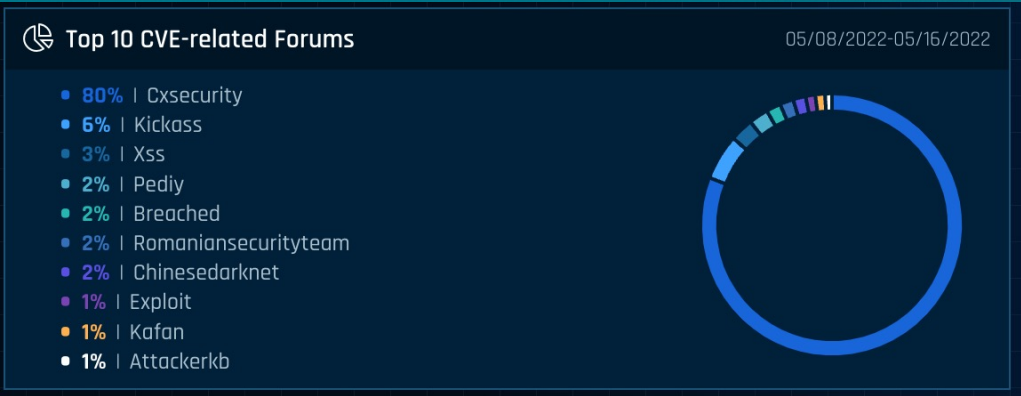
Show 16 duplicates

Order by

Results: 50

page 1 of 17

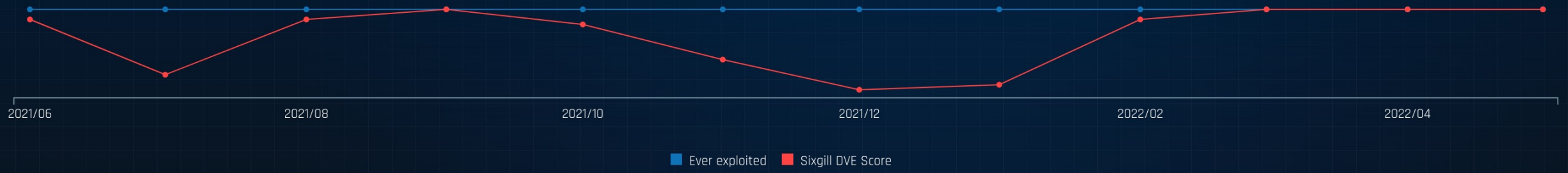
Vulnerability Prioritization Using Dark Web Intelligence (Windows EOL)



Attributes | Events | Chart | Github | References

Date	Current Score	Previously Exploited Score	Description
05/14/2022	10	10	Mentioned on clear web twitter 9b0f46f45bc4a5475858d3845034b4e7d0eeff85
05/14/2022	10	10	Mentioned on twitter (highly regarded source with rank 4.0. 9b0f46f45bc4a5475858d3845034b4e7d0eeff85
05/13/2022	10	10	Mentioned on clear web twitter 4f646257d40062ee53a0c62c9f8be5c54ca3f1d1

Attributes | Events | Chart | Github | References



Conduct Security Vulnerability Prioritization vs. Analysis

Combine other sources like CTI with traditional VM

Integrate external sources and metrics to add risk measure to existing vulnerability management techniques

Continually measure your risk

Continually assess CVE-related external risks to re-prioritize system patch management personnel and efforts

Enrich your risk analysis

Incorporate broader threat intelligence from all depths of the web and uncover the real threat to your CDE

Risk-based Vulnerability Prioritization

Grazie!

Thank You!

PCI Security Standards Council®