



August 2022

REFERENCE IMPLEMENTATION REVISION 1 FOR REPRESENTATION OF CYBER ADVERSARY BEHAVIOR IN STRUCTURED THREAT INFORMATION EXCHANGE (STIX) FORMAT

Prepared by:

The Johns Hopkins University
Applied Physics Laboratory
11100 Johns Hopkins Rd.
Laurel, Maryland 20723-6099

Authors:

Charles Frick, Charles.Frick@jhuapl.edu

Tim Zhan



APL Research Team

- Suzanne Hassell
- Kurt Karolenko
- Jason O'Connor
- Timotius Oentung
- Ali Shahegh

Prepared for: The Cybersecurity and Infrastructure Security Agency

Distribution Statement A. Approved for public release: distribution unlimited.

Disclaimer: The views and conclusions contained in this document are those of the author and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security / Cybersecurity and Infrastructure Security Agency.

CONTENTS

1. Introduction 4

2. Behavior sharing research 4

 2.1 Motivation for the Research 4

 2.2 Research Environment..... 4

 2.3 Initial Behavior Set Reference Implementation 6

3. Next steps 24

4. Conclusion..... 24

5. Appendix A: Acronymns..... 25

6. Appendix B: Complete behavior set STIX bundle..... 26

FIGURES

Figure 1: APL Reference Implementation Research Environment 5

Figure 2: Reference Implementation Emulated Attack Scenario 7

Figure 3: Visualization of Reference Implementation Behavior Set STIX Bundle 9

Figure 4: Simplified Example of Adversary Behaviors 16

Figure 5: Conceptual Process for Detection Correlation Logic 20

1. INTRODUCTION

The Johns Hopkins University Applied Physics Laboratory (APL), under the sponsorship of the Cybersecurity and Infrastructure Security Agency (CISA), seeks to dramatically change the timeline and effectiveness of cyber defense via integration, automation, and information sharing. Towards this goal, APL is providing a reference implementation for our research into machine readable objects, in Structured Threat Information eXchange (STIX)¹ format, to represent cyber adversary behaviors on a network. This report provides an overview of the research methodology as well as a guide for understanding the content and concepts within the reference implementation object.

2. BEHAVIOR SHARING RESEARCH

The key focus of APL's adversary behavior research is the generation of machine readable objects to represent adversary behavior on a target network. This is an evolution of previous APL research conducted for CISA and as part of the Integrated Adaptive Cyber Defense (IACD)² framework.

Previous research focused on designing the proper format to hold adversary behavior. The use of custom objects within STIX standard version 2.1 was the format chosen based on those efforts. For this reference implementation, APL research focused on the creation of the content for a robust machine readable STIX bundle that could be shared throughout a community. This design allows both human analysts and automation to use the shared information to detect an adversary's observed behavior within the victim network.

2.1 Motivation for the Research

Previous APL work under the IACD program identified a significant gap in Cyber Threat Intelligence (CTI) sharing when that sharing is solely focused on Indicators of Compromise (IOCs). IOCs by their very nature have a limited time window of being actionable towards network defense. While significant progress with Security Orchestration, Automation and Response (SOAR) has been achieved to take action on IOCs within a viable timeline for network defense, there remains a clear need for sharing data that can help a community of network defenders proactively defend against advanced attacks.

2.2 Research Environment

APL maintains a robust virtualization testbed environment to support our research and experimentation efforts. Figure 1 provides a summary of how a dedicated enclave of that environment was configured for the development of the reference implementation.

¹ <https://oasis-open.github.io/cti-documentation/>

² <https://iacdautomate.org>

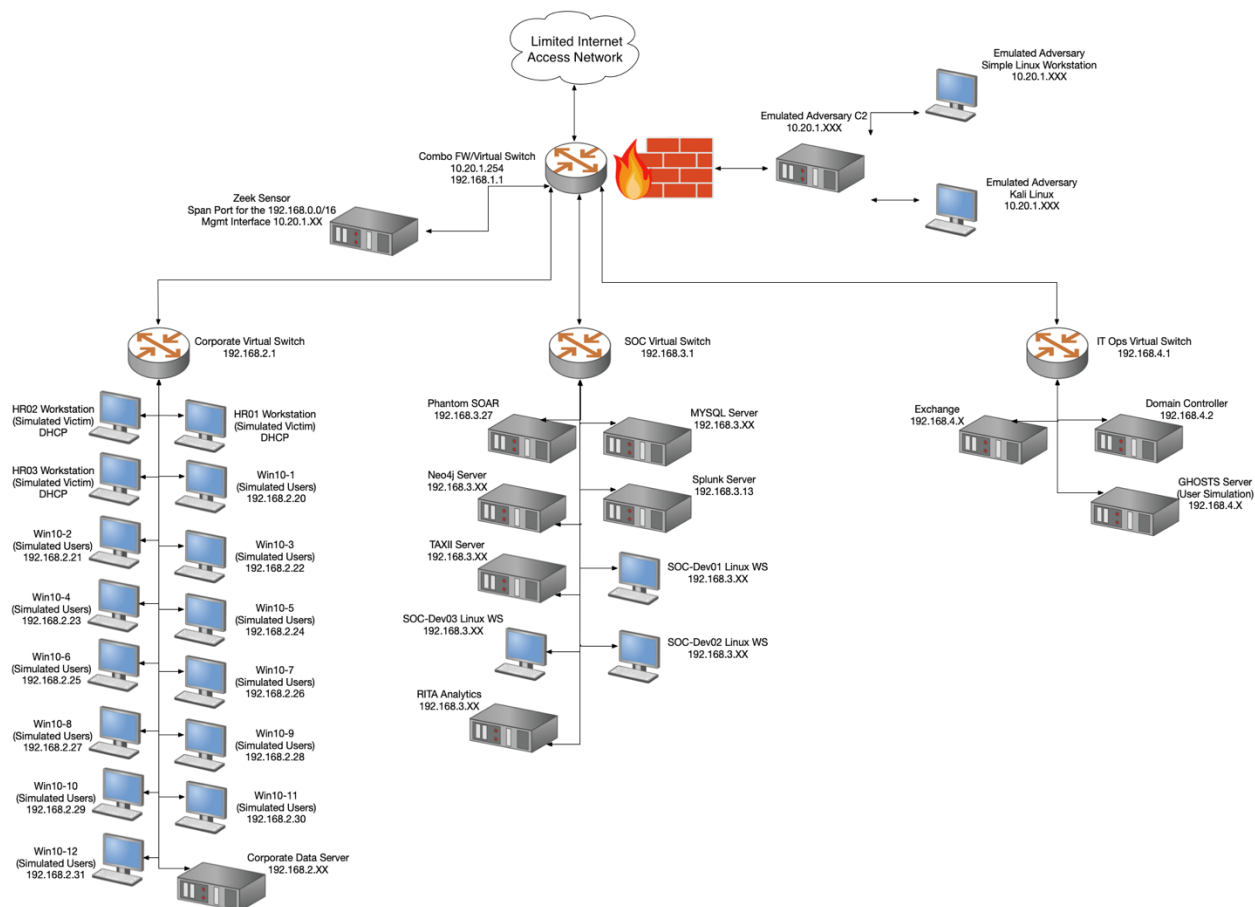


Figure 1: APL Reference Implementation Research Environment

The research environment is sectioned into four main enclaves. The following description of the enclaves provides an overview of the tools used in creation of the reference implementation but is not provided as any form of endorsement for any singular technology or open source project:

- An emulated adversary enclave implementing common threat emulation tools such as Cobalt Strike³
- An emulated corporate enclave containing:
 - Windows workstations automated with the Carnegie Mellon University (CMU) GHOSTS⁴ agent to create benign user activity within the network
 - Splunk⁵ Security Information and Event Management (SIEM) forwarders for SYSMON⁶ and Windows event logs
 - A file server to contain emulated sensitive information that would be the adversary's target for data exfiltration

³ <https://www.cobaltstrike.com>

⁴ <https://github.com/cmu-sei/GHOSTS>

⁵ <https://www.splunk.com>

⁶ <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

- An emulated Network Operations Center enclave containing:
 - Windows domain controller for Active Directory
 - Exchange email server
 - Command and control for the CMU GHOSTS agents
- An emulated Security Operations Center enclave containing:
 - A Zeek⁷ network sensor to analyze traffic
 - A Trusted Automated eXchange of Indicator Information (TAXII) server for the transmission of any shared STIX objects
 - A MySQL⁸ database server for holding STIX data internally to the network
 - This was done to simulate a very basic Threat Intel Platform (TIP) capability since the research for the reference implementation did not require all the features of a TIP
 - A Real Intelligence Threat Analytics (RITA)⁹ server for generation of beaconing alerts from the Zeek analytics
 - A Splunk SIEM for detecting adversary activity
 - Used in research analysis to develop a shared behavior object
 - Also used from the point of view as a recipient who would receive a bundle and translate that data into analytics for a SIEM
 - A Splunk SOAR platform for automating SOC activities
 - While not heavily used in the reference implementation, work was done to update and use SOAR to support future research on automating the behavior development process as well as executing future correlation and response actions

2.3 Initial Behavior Set Reference Implementation

APL's research focuses on creating STIX "behavior-set" bundles. These bundles represent sequences of observed adversary behaviors within a network that are not dependent on traditional IOCs (file hash, URL, IP address, etc.). Instead, the bundles include detection analytics for individual behaviors as well as information on how to correlate behaviors to better detect and prioritize a sequence of observed adversary behaviors.

Bundles such as the reference implementation are intended to augment a larger set of CTI within the STIX standard. As behaviors represent sequences of procedures conducted by an adversary, they are inherently linked to adversary tactics and techniques, represented within the MITRE ATT&CK^{®10} framework. The goal of the behavior sets and detection bundles is to provide more actionable detection techniques than those present in the ATT&CK description. Achieving this goal will make it easier for community and vendors to rapidly add detections for advanced attacks that could assist with defense against multiple campaigns by a cyber adversary or set of adversaries.

⁷ <https://github.com/zeek/zeek>

⁸ <https://www.mysql.com>

⁹ <https://github.com/activecm/rita>

¹⁰ <https://attack.mitre.org>

A summary of the overall goals for the reference implementation research follows:

- Emulate threat behaviors
- Identify and create behavior objects
- Correlate behavior objects into behavior sets
- Create detection objects for behavior sets
- Develop a STIX bundle to include:
 - Behavior Set
 - Observables
 - Detections
- Store and share the STIX bundle

2.3.1 Adversary Scenario

To properly capture a realistic set of adversary behaviors, APL required a representative sample adversary attack. Figure 2 provides a visual representation of the sample attack that was based on the “APT 37/Reaper”¹¹ campaign.

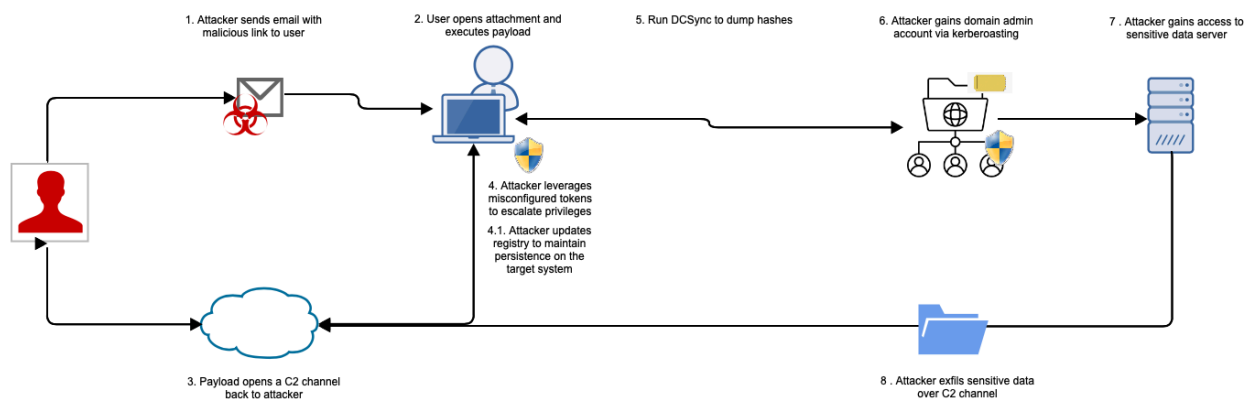


Figure 2: Reference Implementation Emulated Attack Scenario

The overall steps in this attack include:

1. Attacker sends an email to the target organization with a malicious link.
2. The user opens the attachment and executes a malicious office macro payload.
 - The details of the file are traditionally shared as IOCs, but those details are often modified rapidly by the attacker, reducing the effectiveness of the IOC in enabling network defense across a community.
3. The payload establishes a command and control (C2) channel to adversary infrastructure.
 - The domains and/or IP addresses of the C2 server are traditionally shared as IOCs, but those details are often modified rapidly by the attacker, reducing the effectiveness of the IOC in enabling network defense across a community.
4. The attacker escalates privileges on the initial victim machine.

¹¹ https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

- The attacker leverages misconfigured tokens to escalate privileges.
 - The attacker then updates the initial victim machine registry to maintain persistence.
5. The attacker uses the "DCSync"¹² capability to retrieve password hashes from the target network's domain controller.
 6. The attacker then uses the "kerberoasting"¹³ technique to gain access as a domain administrator account.
 7. The attacker uses this compromised administrator account to gain access to a sensitive data server.
 8. The attacker then exfiltrates sensitive data via the established C2 channel.

2.3.2 Behavior Set STIX Bundle

The full text of the reference implementation STIX bundle for representing an adversary set of behaviors is provided in [Appendix B](#). Figure 3 provides a visualization of the bundle via the STIX visualizer from the OASIS standards group.¹⁴

¹² <https://attack.mitre.org/techniques/T1003/006/>

¹³ <https://attack.mitre.org/techniques/T1558/003/>

¹⁴ <https://oasis-open.github.io/cti-stix-visualization/>

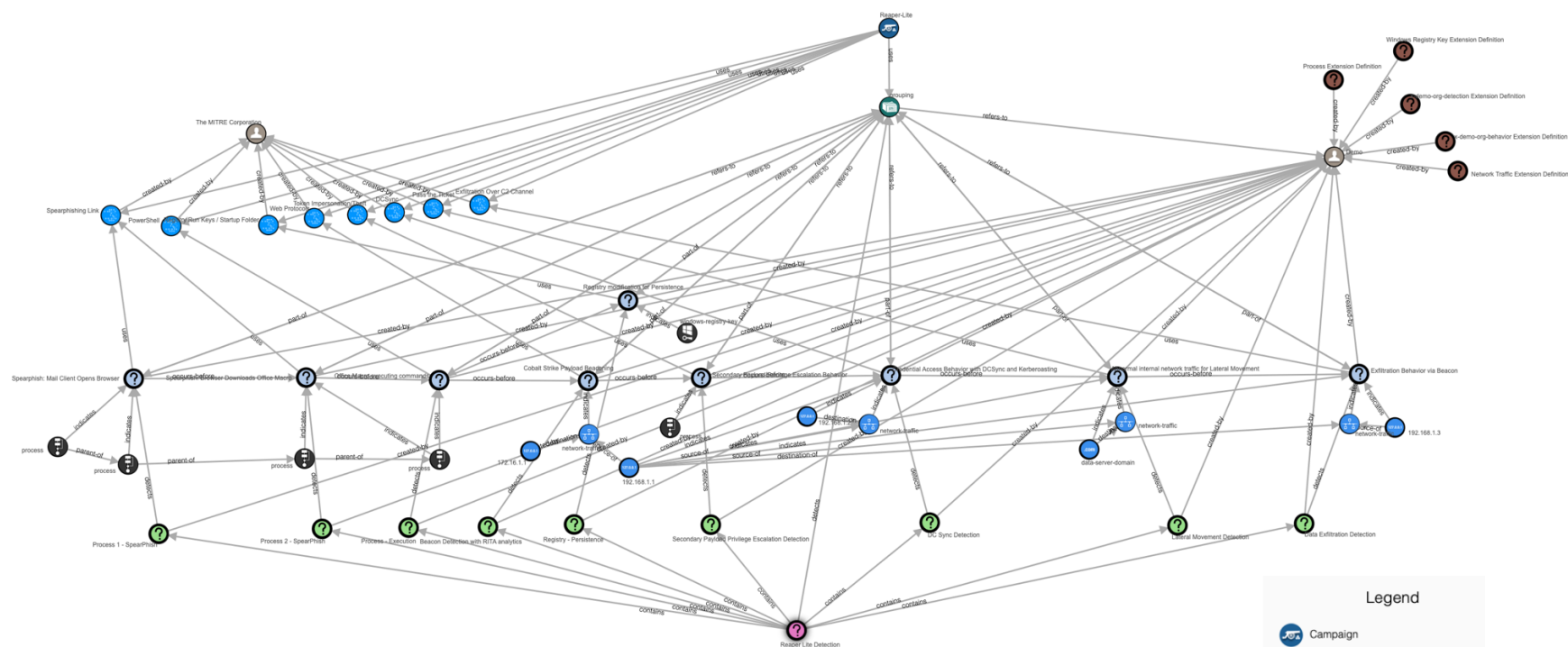











Figure 3: Visualization of Reference Implementation Behavior Set STIX Bundle

This reference implementation bundle contains several custom SDOs as well as several custom SCOs. The standard SDO of a “grouping” object was used to represent the observed set of behaviors. The following descriptions of the custom objects provides a key for reading the diagram in Figure 3 with respect to the custom objects:



- Behavior SDO
 - Icon: 
 - Description: Behavior SDOs represent the observed adversary behaviors within a particular campaign. These consist of a sequence of actions characterized by multiple techniques (and sub-techniques) in pursuit of multiple tactical goals. As such, these objects may contain relationships to STIX Attack-Pattern SDOs that are traditionally used to represent entries in the MITRE ATT&CK framework. These objects exist to provide more actionable data for detection and response than what is currently found in the ATT&CK information.
 - Fields within the object:
 - STIX type
 - STIX specification version
 - STIX ID
 - Created by reference
 - Created date
 - Modification date
 - Name
 - Tactic
 - Technique
 - First seen date
 - Platforms affected by the behavior
 - Extensions
- Detection SDO
 - Icon: 
 - Description: Detection SDOs provide information on how to detect a particular behavior observed from a campaign. These detections are presented as analytics referencing the SCOs related to the behavior object. The key distinction is that the analytics are designed to not be IOC specific so that they can relate to multiple occurrences of the behavior. It is possible to have more than a single detection for a behavior. The guidance on how to correlate these detections within a set of behaviors is defined in the Detection Group SDO.
 - Fields within the object:
 - STIX type
 - STIX specification version
 - STIX ID
 - Created by reference
 - Created date
 - Modification date
 - Name

- Analytic for detection
- Data sources to support analytic
- Detection Group SDO
 - Icon: 
 - Description: The Detection Group SDO is intended to provide the guidance on how to correlate the multiple detections within a grouping of behavior SDOs. As of Spiral 26, APL is still refining the logic and required metadata for strong correlations but the version provided in the Spiral 26 reference implementation conveys the current status of the object.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Created date
 - Modification date
 - Name
 - Description field
 - Correlation workflows describing the correlation procedure
 - List of detection object STIX IDs to use for correlation
- Identity SDO
 - Icon: 
 - Description: The Identity SDO represents entities relevant to the CTI held in the bundle. The bundle contains an Identity SDO for MITRE Corporation, which produced the Attack-Pattern SDOs. The bundle also contains an Identity SDO for the targeted organization.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Created date
 - Modification date
 - Name
- Grouping SDO
 - Icon: 
 - Description: The Grouping SDO is used to associate related STIX objects together. A Grouping SDO is used to group the Behavior SDOs observed during the attack.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Created date
 - Modification date



- Context on how the objects within the Grouping are related
 - References to objects within grouping
- Attack-Pattern SDO
 - Icon: 
 - Description: The Attack-Pattern SDO describes adversary tactics, techniques, and procedures (TTPs). The Attack-Pattern SDOs in the bundle have been constructed by MITRE and include custom fields.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Name
 - Description field
 - Created by
 - Created date
 - Modification date
 - Kill chain phases
 - Object marking references
 - External references
 - MITRE custom fields
 - Data sources
 - MITRE version
 - Platforms
 - Flag to determine if the instance is a sub technique
 - Contributors
 - MITRE detection
 - MITRE ATT&CK specification version
 - Domains
 - Modified by Identity reference
- Campaign SDO
 - Icon: 
 - Description: The Campaign SDO groups adversarial activity against specific targets over a period of time. The object is used to group the Attack-Pattern SDOs involved in the attack. In the bundle, the Campaign SDO also refers to the Grouping SDO containing the Behavior SDOs.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Created date
 - Modification date
 - Name
 - Description field
 - First seen date

- Last seen date
- Process SCO
 - Icon: 
 - Description: Process SCOs are used for observed sequences of processes executed within an observed behavior. These is often low-level information found within target network log sources such as SYSMON¹⁵. As opposed to traditional IoCs that may represent the name of a particular malicious process, these SCOs capture common processes within multiple target environments to describe when one process is creating a new process. For example, this is used to capture when something like office applications spawn new processes such as PowerShell or Windows Command Line via a malicious macro. The sequence of Process SCOs is key to developing the detection object for the behavior of new system process creation.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Object marking refs
 - Granular markings
 - Flag to determine whether the referenced information in the process is “defanged”
 - Flag to determine if the SCO is hidden
 - Process ID (PID)
 - Created date
 - Current Working Directory (CWD)
 - Command line information for the process when available
 - Opened connection references
 - Creator user reference
 - Object reference to executable binary executed as the process image
 - Object reference to parent process
 - Object references to child processes
 - Extensions applied to the SCO
 - Action
 - User
 - Source
 - Creator process name: list of process names or patterns that may spawn the current process
 - New process name: list of process names or patterns that the creator processes may create
 - Windows event code
- Registry SCO
 - Icon: 

¹⁵ <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

- Description: The registry key SCO provides details for adversary behaviors that modify a particular registry key. It is intended to help restrict behavior alerts to adversary campaigns that modify a specify Windows Registry key. By linking it to the processes created within a chain of Process SCOs, detection is improved. The goal is to share the correlating fact that the process created by a chain of process SCOs is the same one that calls to the registry to make this change. This is different than sharing the name of a specific process from a single incident that calls “regedit.exe” as it provides the path to identify new processes in new campaigns.
- Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Registry key referenced
 - Registry key values
 - Extensions applied to SCO
 - Action performed on the key
 - New value of the key
 - ID of process that acted on the key
 - Name of process that acted on the key
- IPv4 Address SCO
 - Icon: 
 - Description: The IPv4 Address SCO represents an IPv4 address.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Value
- Network Traffic SCO
 - Icon: 
 - Description: The Network Traffic SCO represents network traffic between a source and destination.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Source IP reference
 - Destination IP reference
 - Protocols
 - Extensions applied to SCO
 - Number of connections
 - Real Intelligence Threat Analysis (RITA¹⁶) score

¹⁶ <https://github.com/activecm/rita>

- Domain Name SCO
 - Icon: 
 - Description: The Domain Name SCO provides observable information of a domain utilized by threat activity
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Domain Value
- Real Intelligence Threat Analysis (RITA¹⁷) score
- Extension Definition SDO
 - Icon: 
 - Description: When custom extensions are added to an SDO, the Extension Definition SDO provides a reference to the JSON schema used to represent the additional data.
 - Fields within the object:
 - STIX type
 - STIX specification version
 - STIX ID
 - Created by reference
 - Created date
 - Modification date
 - Name
 - Link to extension schema
 - Version
 - List of extension types

2.3.3 Detailed Example for a Subset of the Behavior Bundle

A detailed subset of the first three observed behaviors from the reference implementation scenario shown in Figure 3 follows to better clarify the concepts and capabilities present within the behavior bundle. This example is intended to demonstrate how information in the shared behavior bundle can aid in detecting the sequence of attacker activities represented in Figure 4.

¹⁷ <https://github.com/activecm/rita>

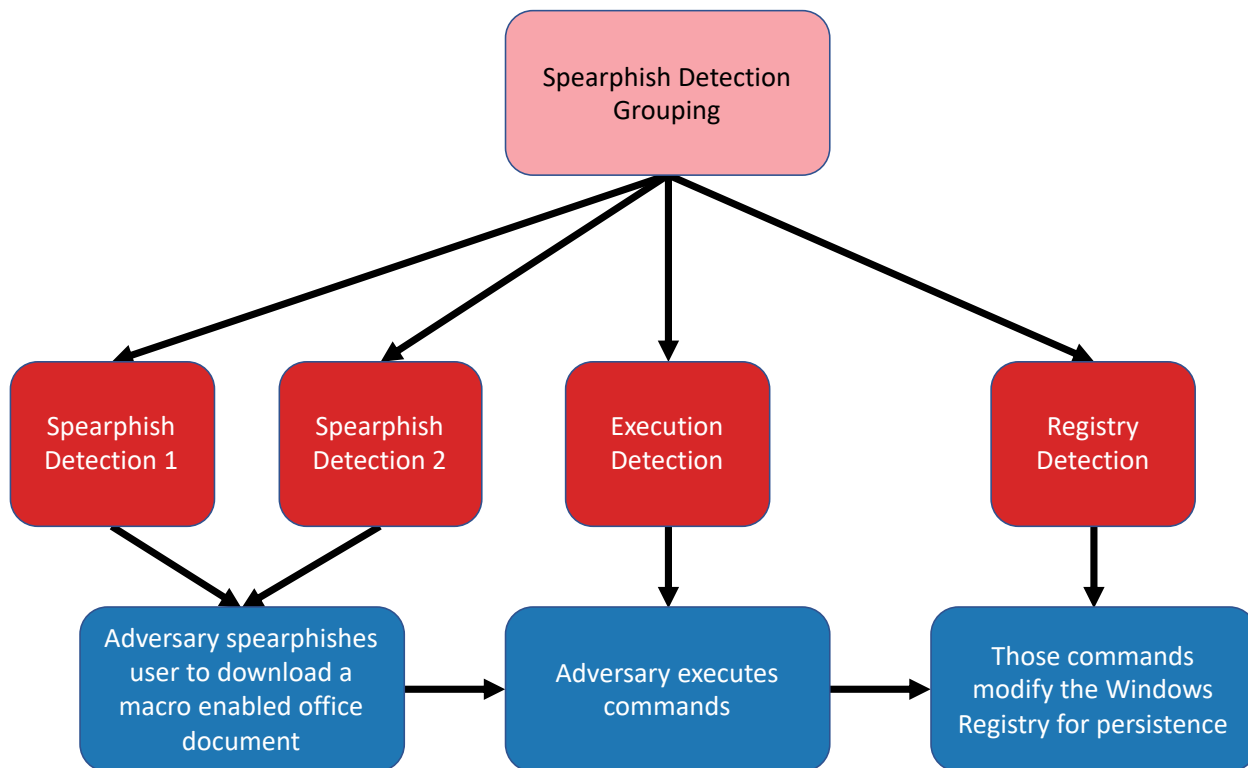


Figure 4: Simplified Example of Adversary Behaviors

The first behavior is intended to represent the observable characteristics within the victim's network when a specific machine's email client (e.g., MS Mail, Outlook, Thunderbird, etc.) spawns a process to open a web browser (e.g., Chrome, Firefox, Edge, etc.) and download a macro-enabled office document (e.g., *.docm, *.pptm, *.xlsm). The specific types of processes observed in the behavior are common within multiple organizations using similar software. These processes can be commonly recorded via standard Microsoft Windows Log types, such as Windows Event Log and SYSMON. The behavior object also contains a link to a pair of analytics to determine this type of behavior. APL chose the Sigma¹⁸ common analytic format for log analysis to represent these connected analytics.

For the detection the email client opening a web browser, the following Sigma rule is provided:

```

---
date: 2021/06/07
detection:
  selection:
    EventCode: '4688'
    Creator_Process_Name|contains:
      - outlook
      - thunderbird
      - mail
    New_Process_Name|contains:

```

¹⁸ <https://github.com/SigmaHQ/sigma>

- edge
- chrome
- firefox

condition: selection
level: high
author: demo
description: Detects Office macro opening from browser.
id: spearphishing
falsepositives:
- Low
title: Spearphishing with Link
logsource:
 index: main
 product: windows
 category: process_event
status: experimental
tags:
- attack.initial_access
- attack.t1566.002

For the detection of the web browser downloading a macro-enabled office document, the following Sigma rule is provided:

date: 2021/06/07
detection:
 selection:
 Process_Command_Line|contains:

- docm
- xlsx
- pptm

 EventCode: '4688'
 Creator_Process_Name|contains:

- edge
- chrome
- firefox

 New_Process_Name|contains:

- winword
- excel
- powerpoint

 condition: selection
level: high
author: demo
description: Detects Office macro opening from browser.
id: spearphishing
falsepositives:
- Low
title: Spearphishing with Link
logsource:
 index: main
 product: windows

```
category: process_event
status: experimental
tags:
- attack.initial_access
- attack.t1566.002
```

The second behavior represents when the macro executes commands on the file system. It contains STIX Relationship Objects (SRO) to the process identified in the first behavior as well as to a detection object with the following Sigma rule:

```
---
date: 2021/06/07
detection:
  condition: run_macro and (not false_positive)
  run_macro:
    Creator_Process_Name|contains:
      - word
      - powerpoint
      - excel
    New_Process_Name|endswith:
      - ".exe"
      - ".dll"
    EventCode: '4688'
  false_positive:
    New_Process_Name|contains:
      - splwow64
level: high
author: demo
description: Detects Office macro execution
id: execution
falsepositives:
- Low
title: Execution
logsource:
  index: main
  product: windows
  category: process_event
status: experimental
tags:
- attack.execution
- attack.t1059
```

The third behavior object represents observed behaviors for the adversary establishing persistence on the initial target via modification of the Windows registry. It contains SROs to an SCO for the registry modification observed as well as one to a detection object represented in the following Sigma rule:

```
---
date: 2021/06/07
detection:
  selection:
    EventCode: '4657'
    Object_Name|contains:
      - Run
      - Shell Folders
  condition: selection
level: high
author: demo
description: Detects new registry run key created event.
id: registry_persistence
falsepositives:
  - High
title: Registry Run Keys
logsource:
  index: main
  product: windows
  category: registry_event
status: experimental
tags:
  - attack.persistence
  - attack.t1547
```

Any single detection object analytic by itself may not detect the behavior without significant numbers of false positives. The detection grouping is intended to provide the correlation logic to execute all of these queries and include the proper common fields between the queries to further increase the confidence of successfully detecting a behavior.

In the current reference implementation, the detection group object has the ability to contain multiple styles of correlation workflow. For the example provided in the reference implementation, correlation workflows are provided in Collaborative Automated Course of Action Operations (CACAO) format as well as base64 encoded Business Process Modeling Notation (BPMN). Figure 5 provides a visualization of the BPMN workflow when extracted and decoded from the reference implementation.

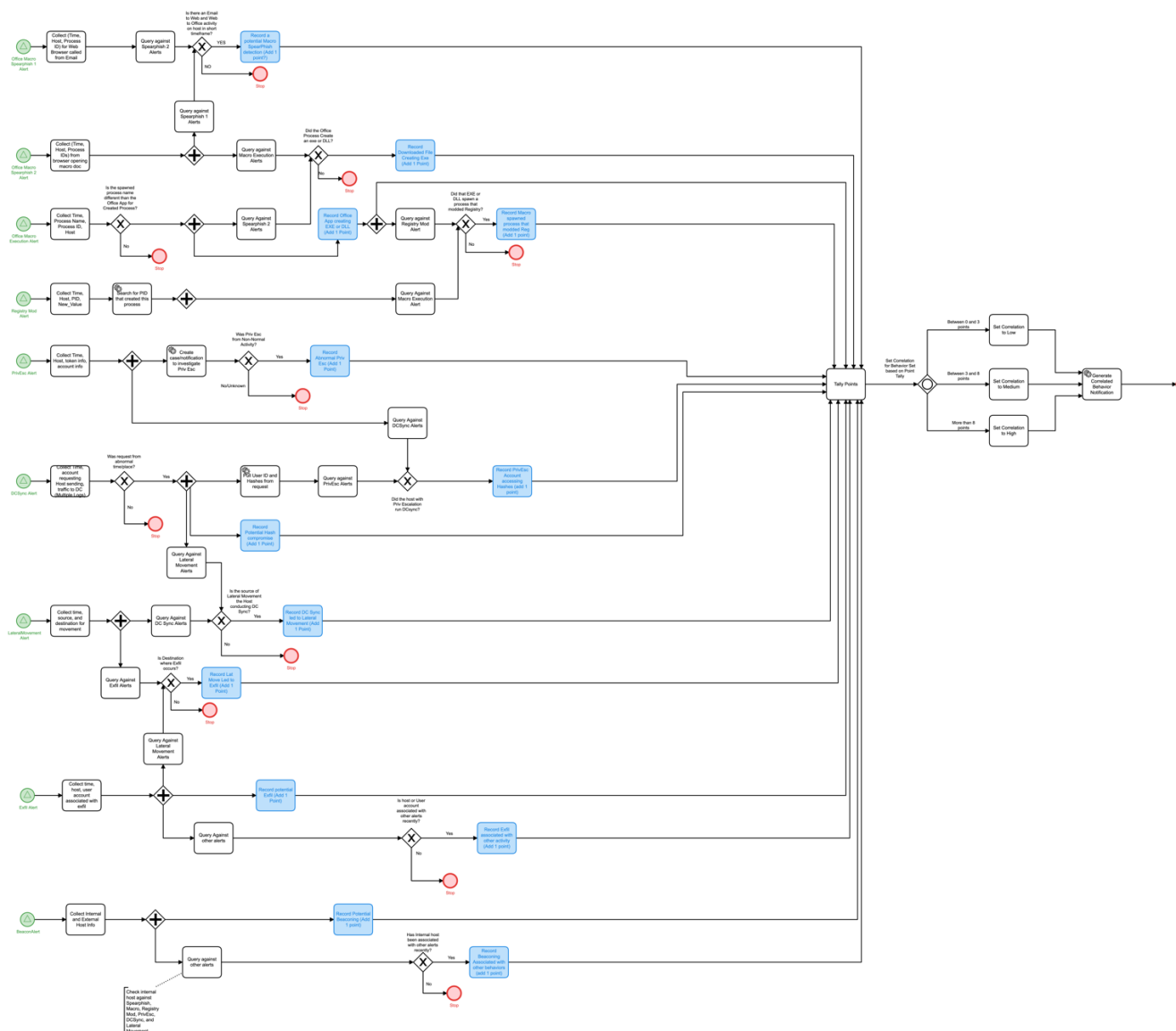


Figure 5: Conceptual Process for Detection Correlation Logic

2.3.4 Using a Received Behavior Set to Augment Network Defense Capability

Once the submitter of a threat intelligence bundle containing behaviors submits the information to a threat feed, the recipient organization can use the correlation information in the detection group to execute the individual queries from each analytic and apply the suggested logic to detect a behavior either automatically or manually, depending on the receiving organization's processes.

It is envisioned that automation will be heavily leveraged to conduct these detections and correlations. This is a key reason for selecting Sigma as there are free and open source tools available to process Sigma rules to translate them to an organization's SIEM of choice. For example, a shared detection analytic from the earlier example:

```
---
date: 2021/06/07
detection:
  selection:
    Process_Command_Line|contains:
      - docm
      - xlsx
      - pptm
    EventCode: '4688'
    Creator_Process_Name|contains:
      - edge
      - chrome
      - firefox
    New_Process_Name|contains:
      - winword
      - excel
      - powerpoint
  condition: selection
level: high
author: demo
description: Detects Office macro opening from browser.
id: spearphishing
falsepositives:
  - Low
title: Spearphishing with Link
logsource:
  index: main
  product: windows
  category: process_event
status: experimental
tags:
  - attack.initial_access
  - attack.t1566.002
```

By providing this analytic in Sigma format, free tools can translate it to a variety of SIEM options that can be selected from the consumer of the bundle. This rule translates automatically into the following Splunk Query:

```
((Process_Command_Line="*docm*" OR Process_Command_Line="*xlsm*" OR
Process_Command_Line="*pptm*") EventCode="4688" (Creator_Process_Name="*edge*" OR
Creator_Process_Name="*chrome*" OR Creator_Process_Name="*firefox*")
(New_Process_Name="*winword*" OR New_Process_Name="*excel*" OR
New_Process_Name="*powerpoint*"))
```

It can also be automatically translated into another SIEM option such as Azure Sentinel:

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "workspace": {
      "type": "String"
    }
  },
  "resources": [
    {
      "id":
        "[concat(resourceId('Microsoft.OperationalInsights/workspaces/providers',
parameters('workspace'),
'Microsoft.SecurityInsights'), '/alertRules/spearphishing')]",
      "name":
        "[concat(parameters('workspace'), '/Microsoft.SecurityInsights/spearphishing')]",
      "type": "Microsoft.OperationalInsights/workspaces/providers/alertRules",
      "apiVersion": "2021-03-01-preview",
      "kind": "Scheduled",
      "properties": {
        "displayName": "Spearphishing with Link by demo",
        "description": "Detects Office macro opening from browser. Technique:
T1566.002.",
        "severity": "high",
        "enabled": true,
        "query": "Windows | where ((Process_Command_Line contains 'docm' or
Process_Command_Line contains 'xlsm' or Process_Command_Line contains 'pptm') and
EventCode == \"4688\" and (Creator_Process_Name contains 'edge' or
Creator_Process_Name contains 'chrome' or Creator_Process_Name contains
'firefox') and (New_Process_Name contains 'winword' or New_Process_Name contains
'excel' or New_Process_Name contains 'powerpoint'))",
        "queryFrequency": "PT30M",
        "queryPeriod": "PT30M",
        "triggerOperator": "GreaterThan",
        "triggerThreshold": 0,
        "suppressionDuration": "PT2H30M",
        "suppressionEnabled": true,
        "tactics": [
```

```

    "InitialAccess"
  ],
  "incidentConfiguration": {
    "createIncident": true,
    "groupingConfiguration": {
      "enabled": false,
      "reopenClosedIncident": false,
      "lookbackDuration": "PT2H30M",
      "matchingMethod": "AllEntities",
      "groupByEntities": [],
      "groupByAlertDetails": [],
      "groupByCustomDetails": []
    }
  },
  "eventGroupingSettings": {
    "aggregationKind": "SingleAlert"
  },
  "alertDetailsOverride": null,
  "customDetails": null,
  "templateVersion": "1.0.0"
}
]
}

```

Sigma is freely available via GitHub¹⁹ and at the time of the reference implementation analysis, the following tools were supported:

- ArcSight
- Azure Sentinel / Azure Log Analytics
- Devo
- ee-outliers
- Elastic X-Pack Watcher
- ElasticSearch Query DSL
- ElasticSearch Query Strings
- Grep with Perl-compatible regular expression support
- Kibana
- LimaCharlie
- LOGIQ
- Logpoint
- LogRhythm
- Microsoft Defender Advanced Threat Protection (MDATP)
- PowerShell
- QRadar
- Qualys
- RSA NetWitness

¹⁹ See section 2.3.4 for link to Sigma GitHub site

- Splunk
- Structured Threat Information Expression (STIX)
- Sumologic
- uberAgent ESA

Once translated into the recipient's SIEM format, these rules can be used to detect the individual behaviors. These detections can then be translated into a series of SIEM alerts that can be forwarded to a new SIEM index. The correlation logic can then be transformed into an operational workflow (either manually executed or executed via automation) that can execute the correlation check when new alerts are generated. Once a medium or high confidence correlation is observed, a security operator can be notified to investigate the potential behavior sequence detection.

3. NEXT STEPS

The next phase of this research will begin investigating the data structure needs to communicate triggers for response Courses of Action (COA), and ways to represent both the triggers and suggested response workflows within additional STIX objects. Additionally, inputs from the greater cyber defense and cyber threat intelligence community will be welcomed to advance the concepts set forth in the reference implementation.

4. CONCLUSION

APL provides this reference implementation and report to facilitate collaboration on research regarding machine readable representations of adversary behavior and to share our work with the larger cyber defense community in the hope that the community can collectively accelerate development of capabilities to defend against the ever growing speed and scale of cyber threat. For any questions regarding this report, please contact the author via email (Charles.Frick@jhuapl.edu).

5. APPENDIX A: ACRONYMS

APL	Johns Hopkins University Applied Physics Laboratory
BPMN	Business Process Modeling Notation
C2	Command and Control
CACAO	Collaborative Automated Course of Action Operations
CISA	Cybersecurity and Infrastructure Security Agency
CMU	Carnegie Mellon University
COA	Courses of Action
CTI	Cyber Threat Intelligence
CUI	Controlled Unclassified Information
CWD	Current Working Directory
IACD	Integrated Adaptive Cyber Defense
IOC	Indicator of Compromise
JSON	JavaScript Object Notation
MDATP	Microsoft Defender Advanced Threat Protection
PID	Process ID
RITA	Real Intelligence Threat Analytics
SCO	STIX Cyber Observables
SDO	STIX Domain Object
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SRO	STIX Relationship Object
STIX	Structured Threat Information eXchange
TAXII	Trusted Automated eXchange of Indicator Information
TIP	Threat Intel Platform

6. APPENDIX B: COMPLETE BEHAVIOR SET STIX BUNDLE

```
{
  "TYPE": "BUNDLE",
  "ID": "BUNDLE--9EDB6354-D73F-4BA2-B774-3D76C6474B14",
  "OBJECTS": [
    {
      "TYPE": "CAMPAIGN",
      "ID": "CAMPAIGN--F3BF3827-D9C5-414D-B0F0-610146FF5D85",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "NAME": "REAPER-LITE",
      "DESCRIPTION": "THIS IS AN EMULATED VERSION OF THE APT37 REAPER CAMPAIGN. IT WAS CREATED TO DEMONSTRATE THE CREATION OF MACHINE READABLE STIX OBJECTS TO REPRESENT ADVERSARY BEHAVIOR.",
      "FIRST_SEEN": "2022-03-31T13:00:00.000Z",
      "LAST_SEEN": "2022-03-31T13:00:00.000Z"
    },
    {
      "TYPE": "X-DEMO-ORG-BEHAVIOR",
      "SPEC_VERSION": "2.1",
      "ID": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AB",
      "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "NAME": "SPEARPHISH: MAIL CLIENT OPENS BROWSER",
      "TACTIC": "INITIAL ACCESS",
      "TECHNIQUE": "T1566.002 SPEARPHISHING LINK",
      "FIRST_SEEN": "2022-03-31T13:00:00.000Z",
      "PLATFORMS": [
        {
          "OPERATING_SYSTEM": "MICROSOFT WINDOWS",
          "VERSION": "10"
        }
      ]
    },
    {
      "EXTENSIONS": {
        "EXTENSION-DEFINITION--9C59FD79-4215-4BA2-920D-3E4F320E1E62": {
          "EXTENSION_TYPE": "NEW-SDO"
        }
      }
    },
    {
      "TYPE": "X-DEMO-ORG-BEHAVIOR",
      "SPEC_VERSION": "2.1",
      "ID": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BC",
      "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "NAME": "SPEARPHISH: BROWSER DOWNLOADS OFFICE MACRO",
      "TACTIC": "INITIAL ACCESS",
      "TECHNIQUE": "T1566.002 SPEARPHISHING LINK",
      "FIRST_SEEN": "2022-03-31T13:00:00.000Z",
      "PLATFORMS": [
        {
          "OPERATING_SYSTEM": "MICROSOFT WINDOWS",
          "VERSION": "10"
        }
      ]
    },
    {
      "EXTENSIONS": {
        "EXTENSION-DEFINITION--9C59FD79-4215-4BA2-920D-3E4F320E1E62": {
          "EXTENSION_TYPE": "NEW-SDO"
        }
      }
    },
    {
      "TYPE": "RELATIONSHIP",
      "SPEC_VERSION": "2.1",
      "ID": "RELATIONSHIP--AE96D1D8-41AB-4BF1-AAD9-6BF704064404",

```

```

"CREATED": "2022-03-31T13:00:00.000Z",
"MODIFIED": "2022-03-31T13:00:00.000Z",
"RELATIONSHIP_TYPE": "USES",
"SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AB",
"TARGET_REF": "ATTACK-PATTERN--2B742742-28C3-4E1B-BAB7-8350D6300FA7"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--AE96D1D8-41AB-4BF1-AAD9-6BF704064404",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "USES",
  "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BC",
  "TARGET_REF": "ATTACK-PATTERN--2B742742-28C3-4E1B-BAB7-8350D6300FA7"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--E38C15BC-224E-4D81-A899-DC3B6F8CEE92",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "USES",
  "SOURCE_REF": "CAMPAIGN--F3BF3827-D9C5-414D-B0F0-610146FF5D85",
  "TARGET_REF": "ATTACK-PATTERN--2B742742-28C3-4E1B-BAB7-8350D6300FA7"
},
{
  "OBJECT_MARKING_REFS": [
    "MARKING-DEFINITION--FA42A846-8D90-4E51-BC29-71D5B4802168"
  ],
  "TYPE": "ATTACK-PATTERN",
  "NAME": "SPEARPHISHING LINK",
  "X_MITRE_DATA_SOURCES": [
    "APPLICATION LOG: APPLICATION LOG CONTENT",
    "NETWORK TRAFFIC: NETWORK TRAFFIC CONTENT",
    "NETWORK TRAFFIC: NETWORK TRAFFIC FLOW"
  ],
  "X_MITRE_VERSION": "2.1",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "KILL_CHAIN_PHASES": [
    {
      "KILL_CHAIN_NAME": "MITRE-ATTACK",
      "PHASE_NAME": "INITIAL-ACCESS"
    }
  ],
  "X_MITRE_PLATFORMS": [
    "LINUX",
    "MACOS",
    "WINDOWS",
    "OFFICE 365",
    "SAAS",
    "GOOGLE WORKSPACE"
  ],
  "X_MITRE_IS_SUBTECHNIQUE": TRUE,
  "ID": "ATTACK-PATTERN--2B742742-28C3-4E1B-BAB7-8350D6300FA7",
  "DESCRIPTION": "ADVERSARIES MAY SEND SPEARPHISHING EMAILS WITH A MALICIOUS LINK IN AN ATTEMPT TO GAIN ACCESS TO VICTIM SYSTEMS. SPEARPHISHING WITH A LINK IS A SPECIFIC VARIANT OF SPEARPHISHING. IT IS DIFFERENT FROM OTHER FORMS OF SPEARPHISHING IN THAT IT EMPLOYS THE USE OF LINKS TO DOWNLOAD MALWARE CONTAINED IN EMAIL, INSTEAD OF ATTACHING MALICIOUS FILES TO THE EMAIL ITSELF, TO AVOID DEFENSES THAT MAY INSPECT EMAIL ATTACHMENTS. SPEARPHISHING MAY ALSO INVOLVE SOCIAL ENGINEERING TECHNIQUES, SUCH AS POSING AS A TRUSTED SOURCE.\N\NALL FORMS OF SPEARPHISHING ARE ELECTRONICALLY DELIVERED SOCIAL ENGINEERING TARGETED AT A SPECIFIC INDIVIDUAL, COMPANY, OR INDUSTRY. IN THIS CASE, THE MALICIOUS EMAILS CONTAIN LINKS. GENERALLY, THE LINKS WILL BE ACCOMPANIED BY SOCIAL ENGINEERING TEXT AND REQUIRE THE USER TO ACTIVELY CLICK OR COPY AND PASTE A URL INTO A BROWSER, LEVERAGING [USER EXECUTION](HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1204). THE VISITED WEBSITE MAY COMPROMISE THE WEB BROWSER USING AN EXPLOIT, OR THE USER WILL BE PROMPTED TO DOWNLOAD APPLICATIONS, DOCUMENTS, ZIP FILES, OR EVEN EXECUTABLES DEPENDING ON THE PRETEXT FOR THE EMAIL IN THE FIRST PLACE. ADVERSARIES MAY ALSO INCLUDE LINKS

```

THAT ARE INTENDED TO INTERACT DIRECTLY WITH AN EMAIL READER, INCLUDING EMBEDDED IMAGES INTENDED TO EXPLOIT THE END SYSTEM DIRECTLY OR VERIFY THE RECEIPT OF AN EMAIL (I.E. WEB BUGS/WEB BEACONS). LINKS MAY ALSO DIRECT USERS TO MALICIOUS APPLICATIONS DESIGNED TO [STEAL APPLICATION ACCESS TOKEN](HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1528)S, LIKE OAUTH TOKENS, IN ORDER TO GAIN ACCESS TO PROTECTED APPLICATIONS AND INFORMATION.(CITATION: TREND MICRO PAWN STORM OAUTH 2017)",

```
"X_MITRE_CONTRIBUTORS": [
  "PHILIP WINTHER",
  "SHAILESH TIWARY (INDIAN ARMY)",
  "MARK WEE",
  "JEFF SAKOWICZ, MICROSOFT IDENTITY DEVELOPER PLATFORM SERVICES (IDPM SERVICES)",
  "SAISHA AGRAWAL, MICROSOFT THREAT INTELLIGENT CENTER (MSTIC)"
],
"X_MITRE_DETECTION": "URL INSPECTION WITHIN EMAIL (INCLUDING EXPANDING SHORTENED LINKS) CAN HELP
DETECT LINKS LEADING TO KNOWN MALICIOUS SITES. DETONATION CHAMBERS CAN BE USED TO DETECT THESE LINKS AND
EITHER AUTOMATICALLY GO TO THESE SITES TO DETERMINE IF THEY'RE POTENTIALLY MALICIOUS, OR WAIT AND CAPTURE
THE CONTENT IF A USER VISITS THE LINK.\N\FILTERING BASED ON DKIM+SPF OR HEADER ANALYSIS CAN HELP DETECT
WHEN THE EMAIL SENDER IS SPOOFED.(CITATION: MICROSOFT ANTI SPOOFING)(CITATION: ACSC EMAIL
SPOOFING)\N\BECAUSE THIS TECHNIQUE USUALLY INVOLVES USER INTERACTION ON THE ENDPOINT, MANY OF THE
POSSIBLE DETECTIONS TAKE PLACE ONCE [USER EXECUTION](HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1204) OCCURS.",
"CREATED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5",
"EXTERNAL_REFERENCES": [
  {
    "URL": "HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1566/002",
    "EXTERNAL_ID": "T1566.002",
    "SOURCE_NAME": "MITRE-ATTACK"
  },
  {
    "URL": "HTTPS://CAPEC.MITRE.ORG/DATA/DEFINITIONS/163.HTML",
    "EXTERNAL_ID": "CAPEC-163",
    "SOURCE_NAME": "CAPEC"
  },
  {
    "URL": "HTTPS://BLOG.TRENDMICRO.COM/TRENDLABS-SECURITY-INTELLIGENCE/PAWN-STORM-ABUSES-OPEN-
AUTHENTICATION-ADVANCED-SOCIAL-ENGINEERING-ATTACKS",
    "DESCRIPTION": "HACQUEBORD, F.. (2017, APRIL 25). PAWN STORM ABUSES OPEN AUTHENTICATION IN
ADVANCED SOCIAL ENGINEERING ATTACKS. RETRIEVED OCTOBER 4, 2019.",
    "SOURCE_NAME": "TREND MICRO PAWN STORM OAUTH 2017"
  },
  {
    "URL": "HTTPS://DOCS.MICROSOFT.COM/EN-US/MICROSOFT-365/SECURITY/OFFICE-365-SECURITY/ANTI-
SPOOFING-PROTECTION?VIEW=0365-WORLDWIDE",
    "DESCRIPTION": "MICROSOFT. (2020, OCTOBER 13). ANTI-SPOOFING PROTECTION IN EOP. RETRIEVED
OCTOBER 19, 2020.",
    "SOURCE_NAME": "MICROSOFT ANTI SPOOFING"
  },
  {
    "URL": "HTTPS://WWW.CYBER.GOV.AU/SITES/DEFAULT/FILES/2019-
03/SPOOF_EMAIL_SENDER_POLICY_FRAMEWORK.PDF",
    "DESCRIPTION": "AUSTRALIAN CYBER SECURITY CENTRE. (2012, DECEMBER). MITIGATING SPOOFED EMAILS
USING SENDER POLICY FRAMEWORK. RETRIEVED OCTOBER 19, 2020.",
    "SOURCE_NAME": "ACSC EMAIL SPOOFING"
  }
],
"SPEC_VERSION": "2.1",
"X_MITRE_ATTACK_SPEC_VERSION": "2.1.0",
"X_MITRE_DOMAINS": [
  "ENTERPRISE-ATTACK"
],
"X_MITRE_MODIFIED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5"
},
{
  "TYPE": "X-DEMO-ORG-BEHAVIOR",
  "SPEC_VERSION": "2.1",
  "ID": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AA",
  "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "OFFICE MACRO EXECUTING COMMANDS",
```

```

    "TACTIC": "EXECUTION",
    "TECHNIQUE": "T1059.001 COMMAND/SCRIPT EXECUTION - VBA",
    "FIRST_SEEN": "2022-03-31T13:00:00.000Z",
    "PLATFORMS": [
      {
        "OPERATING_SYSTEM": "MICROSOFT WINDOWS",
        "VERSION": "10"
      }
    ],
    "EXTENSIONS": {
      "EXTENSION-DEFINITION--9C59FD79-4215-4BA2-920D-3E4F320E1E62": {
        "EXTENSION_TYPE": "NEW-SDO"
      }
    }
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--399EE227-E888-4DCD-BBC8-B79CF5CFF259",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "USES",
    "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AA",
    "TARGET_REF": "ATTACK-PATTERN--970A3432-3237-47AD-BCCA-7D8CBB217736"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--81DA5956-D9EA-4A09-9E3D-AB09BE3CC3EB",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "USES",
    "SOURCE_REF": "CAMPAIGN--F3BF3827-D9C5-414D-B0F0-610146FF5D85",
    "TARGET_REF": "ATTACK-PATTERN--970A3432-3237-47AD-BCCA-7D8CBB217736"
  },
  {
    "TYPE": "ATTACK-PATTERN",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "NAME": "POWERSHELL",
    "X_MITRE_DATA_SOURCES": [
      "COMMAND: COMMAND EXECUTION",
      "MODULE: MODULE LOAD",
      "PROCESS: PROCESS CREATION",
      "SCRIPT: SCRIPT EXECUTION"
    ],
    "X_MITRE_VERSION": "1.1",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "X_MITRE_CONTRIBUTORS": [
      "PRAETORIAN"
    ],
    "ID": "ATTACK-PATTERN--970A3432-3237-47AD-BCCA-7D8CBB217736",
    "X_MITRE_PLATFORMS": [
      "WINDOWS"
    ],
    "X_MITRE_IS_SUBTECHNIQUE": TRUE,
    "X_MITRE_PERMISSIONS_REQUIRED": [
      "USER",
      "ADMINISTRATOR"
    ],
    "DESCRIPTION": "ADVERSARIES MAY ABUSE POWERSHELL COMMANDS AND SCRIPTS FOR EXECUTION. POWERSHELL IS A POWERFUL INTERACTIVE COMMAND-LINE INTERFACE AND SCRIPTING ENVIRONMENT INCLUDED IN THE WINDOWS OPERATING SYSTEM. (CITATION: TECHNET POWERSHELL) ADVERSARIES CAN USE POWERSHELL TO PERFORM A NUMBER OF ACTIONS, INCLUDING DISCOVERY OF INFORMATION AND EXECUTION OF CODE. EXAMPLES INCLUDE THE <CODE>START-PROCESS</CODE> CMDLET WHICH CAN BE USED TO RUN AN EXECUTABLE AND THE <CODE>INVOKE-COMMAND</CODE> CMDLET WHICH RUNS A COMMAND LOCALLY OR ON A REMOTE COMPUTER (THOUGH ADMINISTRATOR PERMISSIONS ARE REQUIRED TO USE POWERSHELL TO CONNECT TO REMOTE SYSTEMS).\N\NPOWERSHELL MAY ALSO BE USED TO DOWNLOAD AND RUN EXECUTABLES FROM THE INTERNET, WHICH CAN BE EXECUTED FROM DISK OR IN MEMORY WITHOUT TOUCHING DISK.\N\NA NUMBER OF POWERSHELL-BASED OFFENSIVE TESTING TOOLS ARE AVAILABLE, INCLUDING [EMPIRE](HTTPS://ATTACK.MITRE.ORG/SOFTWARE/S0363),

```

[POWERSPLOIT](HTTPS://ATTACK.MITRE.ORG/SOFTWARE/S0194), [POSHC2](HTTPS://ATTACK.MITRE.ORG/SOFTWARE/S0378), AND PSATTACK.(CITATION: GITHUB PSATTACK)\N\NPOWERSHELL COMMANDS/SCRIPTS CAN ALSO BE EXECUTED WITHOUT DIRECTLY INVOKING THE <CODE>POWERSHELL.EXE</CODE> BINARY THROUGH INTERFACES TO POWERSHELL'S UNDERLYING <CODE>SYSTEM.MANAGEMENT.AUTOMATION</CODE> ASSEMBLY DLL EXPOSED THROUGH THE .NET FRAMEWORK AND WINDOWS COMMON LANGUAGE INTERFACE (CLI). (CITATION: SIXDUB POWERPICK JAN 2016)(CITATION: SILENTBREAK OFFENSIVE PS DEC 2015)(CITATION: MICROSOFT PSFROMCSHARP APR 2014)",

```

"OBJECT_MARKING_REFS": [
  "MARKING-DEFINITION--FA42A846-8D90-4E51-BC29-71D5B4802168"
],
"KILL_CHAIN_PHASES": [
  {
    "KILL_CHAIN_NAME": "MITRE-ATTACK",
    "PHASE_NAME": "EXECUTION"
  }
],
"X_MITRE_REMOTE_SUPPORT": TRUE,
"X_MITRE_DETECTION": "IF PROPER EXECUTION POLICY IS SET, ADVERSARIES WILL LIKELY BE ABLE TO DEFINE THEIR OWN EXECUTION POLICY IF THEY OBTAIN ADMINISTRATOR OR SYSTEM ACCESS, EITHER THROUGH THE REGISTRY OR AT THE COMMAND LINE. THIS CHANGE IN POLICY ON A SYSTEM MAY BE A WAY TO DETECT MALICIOUS USE OF POWERSHELL. IF POWERSHELL IS NOT USED IN AN ENVIRONMENT, THEN SIMPLY LOOKING FOR POWERSHELL EXECUTION MAY DETECT MALICIOUS ACTIVITY.\N\NMONITOR FOR LOADING AND/OR EXECUTION OF ARTIFACTS ASSOCIATED WITH POWERSHELL SPECIFIC ASSEMBLIES, SUCH AS SYSTEM.MANAGEMENT.AUTOMATION.DLL (ESPECIALLY TO UNUSUAL PROCESS NAMES/LOCATIONS).(CITATION: SIXDUB POWERPICK JAN 2016)(CITATION: SILENTBREAK OFFENSIVE PS DEC 2015)\N\NIT IS ALSO BENEFICIAL TO TURN ON POWERSHELL LOGGING TO GAIN INCREASED FIDELITY IN WHAT OCCURS DURING EXECUTION (WHICH IS APPLIED TO .NET INVOCATIONS). (CITATION: MALWARE ARCHAEOLOGY POWERSHELL CHEAT SHEET) POWERSHELL 5.0 INTRODUCED ENHANCED LOGGING CAPABILITIES, AND SOME OF THOSE FEATURES HAVE SINCE BEEN ADDED TO POWERSHELL 4.0. EARLIER VERSIONS OF POWERSHELL DO NOT HAVE MANY LOGGING FEATURES.(CITATION: FIREEYE POWERSHELL LOGGING 2016) AN ORGANIZATION CAN GATHER POWERSHELL EXECUTION DETAILS IN A DATA ANALYTIC PLATFORM TO SUPPLEMENT IT WITH OTHER DATA.",
"CREATED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5",
"EXTERNAL_REFERENCES": [
  {
    "URL": "HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1059/001",
    "EXTERNAL_ID": "T1059.001",
    "SOURCE_NAME": "MITRE-ATTACK"
  },
  {
    "SOURCE_NAME": "TECHNET POWERSHELL",
    "DESCRIPTION": "MICROSOFT. (N.D.). WINDOWS POWERSHELL SCRIPTING. RETRIEVED APRIL 28, 2016.",
    "URL": "HTTPS://TECHNET.MICROSOFT.COM/EN-US/SCRIPTCENTER/DD742419.ASPX"
  },
  {
    "SOURCE_NAME": "GITHUB PSATTACK",
    "DESCRIPTION": "HAIGHT, J. (2016, APRIL 21). PS>ATTACK. RETRIEVED JUNE 1, 2016.",
    "URL": "HTTPS://GITHUB.COM/JAREDHAIGHT/PSATTACK"
  },
  {
    "URL": "HTTP://WWW.SIXDUB.NET/?P=367",
    "DESCRIPTION": "WARNER, J.. (2015, JANUARY 6). INEXORABLE POWERSHELL - A RED TEAMER'S TALE OF OVERCOMING SIMPLE APPLOCKER POLICIES. RETRIEVED DECEMBER 8, 2018.",
    "SOURCE_NAME": "SIXDUB POWERPICK JAN 2016"
  },
  {
    "URL": "HTTPS://SILENTBREAKSECURITY.COM/POWERSHELL-JOBS-WITHOUT-POWERSHELL-EXE/",
    "DESCRIPTION": "CHRISTENSEN, L.. (2015, DECEMBER 28). THE EVOLUTION OF OFFENSIVE POWERSHELL INVOCATION. RETRIEVED DECEMBER 8, 2018.",
    "SOURCE_NAME": "SILENTBREAK OFFENSIVE PS DEC 2015"
  },
  {
    "URL": "HTTPS://BLOGS.MSDN.MICROSOFT.COM/KEBAB/2014/04/28/EXECUTING-POWERSHELL-SCRIPTS-FROM-C/",
    "DESCRIPTION": "BABINEC, K. (2014, APRIL 28). EXECUTING POWERSHELL SCRIPTS FROM C#. RETRIEVED APRIL 22, 2019.",
    "SOURCE_NAME": "MICROSOFT PSFROMCSHARP APR 2014"
  },
  {
    "SOURCE_NAME": "MALWARE ARCHAEOLOGY POWERSHELL CHEAT SHEET",
    "DESCRIPTION": "MALWARE ARCHAEOLOGY. (2016, JUNE). WINDOWS POWERSHELL LOGGING CHEAT SHEET - WIN 7/WIN 2008 OR LATER. RETRIEVED JUNE 24, 2016.",

```

```

"URL": "HTTP://WWW.MALWAREARCHAEOLOGY.COM/S/WINDOWS-POWERSHELL-LOGGING-CHEAT-SHEET-VER-JUNE-
2016-V2.PDF"
},
{
  "SOURCE_NAME": "FIREEYE POWERSHELL LOGGING 2016",
  "DESCRIPTION": "DUNWOODY, M. (2016, FEBRUARY 11). GREATER VISIBILITY THROUGH POWERSHELL LOGGING.
RETRIEVED FEBRUARY 16, 2016.",
  "URL": "HTTPS://WWW.FIREEYE.COM/BLOG/THREAT-RESEARCH/2016/02/GREATER_VISIBILITYT.HTML"
}
],
"SPEC_VERSION": "2.1",
"X_MITRE_ATTACK_SPEC_VERSION": "2.1.0",
"X_MITRE_DOMAINS": [
  "ENTERPRISE-ATTACK"
],
"X_MITRE_MODIFIED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5"
},
{
  "TYPE": "X-DEMO-ORG-BEHAVIOR",
  "SPEC_VERSION": "2.1",
  "ID": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BB",
  "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "COBALT STRIKE PAYLOAD BEACONING",
  "TACTIC": "COMMAND AND CONTROL",
  "TECHNIQUE": "T1071.001 - APPLICATION LAYER PROTOCOL - WEB PROTOCOLS",
  "FIRST_SEEN": "2022-03-31T13:00:00.000Z",
  "PLATFORMS": [
    {
      "OPERATING_SYSTEM": "MICROSOFT WINDOWS",
      "VERSION": "10"
    }
  ],
  "EXTENSIONS": {
    "EXTENSION-DEFINITION--9C59FD79-4215-4BA2-920D-3E4F320E1E62": {
      "EXTENSION_TYPE": "NEW-SDO"
    }
  }
},
{
  "TYPE": "IPV4-ADDR",
  "SPEC_VERSION": "2.1",
  "ID": "IPV4-ADDR--57A33521-9761-54A9-81DE-3C11E441D86B",
  "VALUE": "192.168.1.1"
},
{
  "TYPE": "IPV4-ADDR",
  "SPEC_VERSION": "2.1",
  "ID": "IPV4-ADDR--BBA1D187-08FB-5000-AED1-EF055C1DFD24",
  "VALUE": "172.16.1.1"
},
{
  "TYPE": "NETWORK-TRAFFIC",
  "SPEC_VERSION": "2.1",
  "ID": "NETWORK-TRAFFIC--15A157A8-26E3-56E0-820B-0C2A8E553A2C",
  "SRC_REF": "IPV4-ADDR--57A33521-9761-54A9-81DE-3C11E441D86B",
  "DST_REF": "IPV4-ADDR--BBA1D187-08FB-5000-AED1-EF055C1DFD24",
  "PROTOCOLS": [
    "IPV4",
    "TCP",
    "HTTP",
    "HTTPS"
  ],
  "EXTENSIONS": {
    "EXTENSION-DEFINITION--3B7505CE-2A18-496E-AA58-311DAC6C1473": {
      "CONNECTIONS": 4022,
      "SCORE": 0.834,

```

```

        "EXTENSION_TYPE": "PROPERTY-EXTENSION"
    }
},
{
    "TYPE": "X-DEMO-ORG-DETECTION",
    "SPEC_VERSION": "2.1",
    "ID": "X-DEMO-ORG-DETECTION--5899C5CC-CE20-44EE-806E-9F64EBA0B29F",
    "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "NAME": "BEACON DETECTION WITH RITA ANALYTICS",
    "DATA_SOURCES": [
        {
            "LOGNAME": "RITA",
            "CATEGORY": "SHOW-BEACONS",
            "SCORE_NUM": "> 0.7"
        }
    ],
    "ANALYTIC": {
        "RULE":
        "LS0TCMRHDGU6IDIWMJIVMDMVMYTKDGL0BGU6IFJPDGEGQMVHY29UCMLK0IA5MMEYMWJLZI00MTM4LTQWYJYTYTK1NS00OTDIMGNLMUUXN
        TKKC3RHDHVZ0IBLHBLCLMTZW50YWMKZGVZY3JPCHRPB246IERLDGVJDGLVBI0IZWFJB25PBMCGD2L0ACBHI0GHPZ2GGZW5VDWDOIHNJB3J
        LCNRHZ3M6CIAGLSBHDHRRHY2SUY29TBWFUF9HBMRFY29UDHJVBAOGIC0GYXR0YWNRLNQXMDCCXMF1DGHVCJOGZGVTBWPSB2DZB3VYU6C
        IAGCHJVZHVJDDOGCML0YQOGIGLUZGV40IBTYWLUCIAGY2F0ZWDVCNK6IHN0B3CTYMVHY29UCWPKZXRLY3RBPB246CIAGC2VSWN0AW9U0G0
        GICAGC291CMNLDHLWZTOGCMLOYS1SB2DZCIAGICBZY29YZV9UDW18Z3Q6IDAUNWOGIGNVBMRPDGLVB3JOGC2VSWN0AW9UCMZHBNLCG9ZA
        XRPDMVZOGOGIC0GVW5RBM93BGP5XZLBD0GBWVKAXVT",
        "TYPE": "SIGMA RULE - BASE64 ENCODED YAML FILE"
    }
},
{
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--C4CBC936-2936-450F-9E79-CE8E2F795A3D",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "DETECTS",
    "SOURCE_REF": "X-DEMO-ORG-DETECTION--5899C5CC-CE20-44EE-806E-9F64EBA0B29F",
    "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BB"
},
{
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--38CEC97F-5BF1-4F39-A043-B217453D3313",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "INDICATES",
    "SOURCE_REF": "NETWORK-TRAFFIC--15A157A8-26E3-56E0-820B-0C2A8E553A2C",
    "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BB"
},
{
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--258248C6-6363-461A-9B8B-452D0518B2A9",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "USES",
    "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BB",
    "TARGET_REF": "ATTACK-PATTERN--DF8B2A25-8BDF-4856-953C-A04372B1C161"
},
{
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--45DCF923-F8B1-45BF-8788-055A7033D6EE",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "USES",
    "SOURCE_REF": "CAMPAIGN--F3BF3827-D9C5-414D-B0F0-610146FF5D85",

```



```

"TARGET_REF": "ATTACK-PATTERN--DF8B2A25-8BDF-4856-953C-A04372B1C161"
},
{
  "TYPE": "ATTACK-PATTERN",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "WEB PROTOCOLS",
  "X_MITRE_DATA_SOURCES": [
    "NETWORK TRAFFIC: NETWORK TRAFFIC FLOW",
    "NETWORK TRAFFIC: NETWORK TRAFFIC CONTENT"
  ],
  "X_MITRE_VERSION": "1.0",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "X_MITRE_PLATFORMS": [
    "LINUX",
    "MACOS",
    "WINDOWS"
  ],
  "X_MITRE_IS_SUBTECHNIQUE": TRUE,
  "ID": "ATTACK-PATTERN--DF8B2A25-8BDF-4856-953C-A04372B1C161",
  "DESCRIPTION": "ADVERSARIES MAY COMMUNICATE USING APPLICATION LAYER PROTOCOLS ASSOCIATED WITH WEB
TRAFFIC TO AVOID DETECTION/NETWORK FILTERING BY BLENDING IN WITH EXISTING TRAFFIC. COMMANDS TO THE REMOTE
SYSTEM, AND OFTEN THE RESULTS OF THOSE COMMANDS, WILL BE EMBEDDED WITHIN THE PROTOCOL TRAFFIC BETWEEN THE
CLIENT AND SERVER. \N\NPROTOCOLS SUCH AS HTTP AND HTTPS THAT CARRY WEB TRAFFIC MAY BE VERY COMMON IN
ENVIRONMENTS. HTTP/S PACKETS HAVE MANY FIELDS AND HEADERS IN WHICH DATA CAN BE CONCEALED. AN ADVERSARY MAY
ABUSE THESE PROTOCOLS TO COMMUNICATE WITH SYSTEMS UNDER THEIR CONTROL WITHIN A VICTIM NETWORK WHILE ALSO
MIMICKING NORMAL, EXPECTED TRAFFIC. ",
  "OBJECT_MARKING_REFS": [
    "MARKING-DEFINITION--FA42A846-8D90-4E51-BC29-71D5B4802168"
  ],
  "KILL_CHAIN_PHASES": [
    {
      "KILL_CHAIN_NAME": "MITRE-ATTACK",
      "PHASE_NAME": "COMMAND-AND-CONTROL"
    }
  ],
  "X_MITRE_DETECTION": "ANALYZE NETWORK DATA FOR UNCOMMON DATA FLOWS (E.G., A CLIENT SENDING
SIGNIFICANTLY MORE DATA THAN IT RECEIVES FROM A SERVER). PROCESSES UTILIZING THE NETWORK THAT DO NOT
NORMALLY HAVE NETWORK COMMUNICATION OR HAVE NEVER BEEN SEEN BEFORE ARE SUSPICIOUS. ANALYZE PACKET CONTENTS
TO DETECT APPLICATION LAYER PROTOCOLS THAT DO NOT FOLLOW THE EXPECTED PROTOCOL STANDARDS REGARDING SYNTAX,
STRUCTURE, OR ANY OTHER VARIABLE ADVERSARIES COULD LEVERAGE TO CONCEAL DATA.(CITATION: UNIVERSITY OF
BIRMINGHAM C2)\N\NMONITOR FOR WEB TRAFFIC TO/FROM KNOWN-BAD OR SUSPICIOUS DOMAINS. ",
  "CREATED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5",
  "EXTERNAL_REFERENCES": [
    {
      "URL": "HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1071/001",
      "EXTERNAL_ID": "T1071.001",
      "SOURCE_NAME": "MITRE-ATTACK"
    },
    {
      "SOURCE_NAME": "UNIVERSITY OF BIRMINGHAM C2",
      "DESCRIPTION": "GARDINER, J., COVA, M., NAGARAJA, S. (2014, FEBRUARY). COMMAND & CONTROL
UNDERSTANDING, DENYING AND DETECTING. RETRIEVED APRIL 20, 2016.",
      "URL": "HTTPS://ARXIV.ORG/FTP/ARXIV/PAPERS/1408/1408.1136.PDF"
    }
  ],
  "SPEC_VERSION": "2.1",
  "X_MITRE_ATTACK_SPEC_VERSION": "2.1.0",
  "X_MITRE_DOMAINS": [
    "ENTERPRISE-ATTACK"
  ],
  "X_MITRE_MODIFIED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5"
},
{
  "TYPE": "X-DEMO-ORG-BEHAVIOR",
  "SPEC_VERSION": "2.1",
  "ID": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890CC",
  "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
  "CREATED": "2022-03-31T13:00:00.000Z",

```

```

"MODIFIED": "2022-03-31T13:00:00.000Z",
"NAME": "REGISTRY MODIFICATION FOR PERSISTENCE",
"TACTIC": "PERSISTENCE",
"TECHNIQUE": "T1547.001 - AUTOSTART EXECUTION - REGISTRY RUN KEYS / STARTUP FOLDER",
"FIRST_SEEN": "2022-03-31T13:00:00.000Z",
"PLATFORMS": [
  {
    "OPERATING_SYSTEM": "MICROSOFT WINDOWS",
    "VERSION": "10"
  }
],
"EXTENSIONS": {
  "EXTENSION-DEFINITION--9C59FD79-4215-4BA2-920D-3E4F320E1E62": {
    "EXTENSION_TYPE": "NEW-SDO"
  }
}
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--8E796CF6-5401-4A23-9354-59B58155BD5E",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "USES",
  "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890CC",
  "TARGET_REF": "ATTACK-PATTERN--9EFB1EA7-C37B-4595-9640-B7680CD84279"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--7A9AFA0A-0C25-4DEC-8F3D-DB92E213643C",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "USES",
  "SOURCE_REF": "CAMPAIGN--F3BF3827-D9C5-414D-B0F0-610146FF5D85",
  "TARGET_REF": "ATTACK-PATTERN--9EFB1EA7-C37B-4595-9640-B7680CD84279"
},
{
  "TYPE": "ATTACK-PATTERN",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "REGISTRY RUN KEYS / STARTUP FOLDER",
  "X_MITRE_DATA_SOURCES": [
    "WINDOWS REGISTRY: WINDOWS REGISTRY KEY CREATION",
    "WINDOWS REGISTRY: WINDOWS REGISTRY KEY MODIFICATION",
    "FILE: FILE MODIFICATION",
    "COMMAND: COMMAND EXECUTION",
    "PROCESS: PROCESS CREATION"
  ],
  "X_MITRE_VERSION": "1.1",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "KILL_CHAIN_PHASES": [
    {
      "KILL_CHAIN_NAME": "MITRE-ATTACK",
      "PHASE_NAME": "PERSISTENCE"
    },
    {
      "KILL_CHAIN_NAME": "MITRE-ATTACK",
      "PHASE_NAME": "PRIVILEGE-ESCALATION"
    }
  ],
  "X_MITRE_PERMISSIONS_REQUIRED": [
    "ADMINISTRATOR",
    "USER"
  ],
  "X_MITRE_PLATFORMS": [
    "WINDOWS"
  ],
  "X_MITRE_IS_SUBTECHNIQUE": TRUE,

```

```
"ID": "ATTACK-PATTERN--9EFB1EA7-C37B-4595-9640-B7680CD84279",
"DESCRIPTION": "ADVERSARIES MAY ACHIEVE PERSISTENCE BY ADDING A PROGRAM TO A STARTUP FOLDER OR
REFERENCING IT WITH A REGISTRY RUN KEY. ADDING AN ENTRY TO THE \"RUN KEYS\" IN THE REGISTRY OR STARTUP
FOLDER WILL CAUSE THE PROGRAM REFERENCED TO BE EXECUTED WHEN A USER LOGS IN. (CITATION: MICROSOFT RUN KEY)
THESE PROGRAMS WILL BE EXECUTED UNDER THE CONTEXT OF THE USER AND WILL HAVE THE ACCOUNT'S ASSOCIATED
PERMISSIONS LEVEL.\N\nPLACING A PROGRAM WITHIN A STARTUP FOLDER WILL ALSO CAUSE THAT PROGRAM TO EXECUTE
WHEN A USER LOGS IN. THERE IS A STARTUP FOLDER LOCATION FOR INDIVIDUAL USER ACCOUNTS AS WELL AS A SYSTEM-
WIDE STARTUP FOLDER THAT WILL BE CHECKED REGARDLESS OF WHICH USER ACCOUNT LOGS IN. THE STARTUP FOLDER PATH
FOR THE CURRENT USER IS <CODE>C:\USERS\[\USER\]\APPDATA\ROAMING\MICROSOFT\WINDOWS\START
MENU\PROGRAMS\STARTUP</CODE>. THE STARTUP FOLDER PATH FOR ALL USERS IS
<CODE>C:\PROGRAMDATA\MICROSOFT\WINDOWS\START MENU\PROGRAMS\STARTUP</CODE>.\N\nTHE FOLLOWING RUN KEYS
ARE CREATED BY DEFAULT ON WINDOWS SYSTEMS:\N\n*
<CODE>HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN</CODE>\N*
<CODE>HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNONCE</CODE>\N*
<CODE>HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN</CODE>\N*
<CODE>HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNONCE</CODE>\N\nRUN KEYS MAY
EXIST UNDER MULTIPLE HIVES.(CITATION: MICROSOFT WOW6432NODE 2018)(CITATION: MALWAREBYTES WOW6432NODE 2016)
THE <CODE>HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNONCEEX</CODE> IS ALSO
AVAILABLE BUT IS NOT CREATED BY DEFAULT ON WINDOWS VISTA AND NEWER. REGISTRY RUN KEY ENTRIES CAN REFERENCE
PROGRAMS DIRECTLY OR LIST THEM AS A DEPENDENCY. (CITATION: MICROSOFT RUNONCEEX APR 2018) FOR EXAMPLE, IT
IS POSSIBLE TO LOAD A DLL AT LOGON USING A \"DEPEND\" KEY WITH RUNONCEEX: <CODE>REG ADD
HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNONCEEX\0001\DEPEND /V 1 /D
\"C:\TEMP\EVIL[.]\DLL\"</CODE> (CITATION: ODDVAR MOE RUNONCEEX MAR 2018)\N\nTHE FOLLOWING REGISTRY KEYS
CAN BE USED TO SET STARTUP FOLDER ITEMS FOR PERSISTENCE:\N\n*
<CODE>HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\USER SHELL
FOLDERS</CODE>\N* <CODE>HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL
FOLDERS</CODE>\N* <CODE>HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SHELL
FOLDERS</CODE>\N* <CODE>HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\USER
SHELL FOLDERS</CODE>\N\nTHE FOLLOWING REGISTRY KEYS CAN CONTROL AUTOMATIC STARTUP OF SERVICES DURING
BOOT:\N\n*
<CODE>HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNSERVICESONCE</CODE>\N*
<CODE>HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNSERVICESONCE</CODE>\N*
<CODE>HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNSERVICES</CODE>\N*
<CODE>HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNSERVICES</CODE>\N\nUSING POLICY
SETTINGS TO SPECIFY STARTUP PROGRAMS CREATES CORRESPONDING VALUES IN EITHER OF TWO REGISTRY KEYS:\N\n*
<CODE>HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\EXPLORER\RUN</CODE>\N*
<CODE>HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\EXPLORER\RUN</CODE>\N\nT
HE WINLOGON KEY CONTROLS ACTIONS THAT OCCUR WHEN A USER LOGS ON TO A COMPUTER RUNNING WINDOWS 7. MOST OF
THESE ACTIONS ARE UNDER THE CONTROL OF THE OPERATING SYSTEM, BUT YOU CAN ALSO ADD CUSTOM ACTIONS HERE. THE
<CODE>HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON\USERINIT</CODE> AND
<CODE>HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON\SHELL</CODE> SUBKEYS
CAN AUTOMATICALLY LAUNCH PROGRAMS.\N\nPROGRAMS LISTED IN THE LOAD VALUE OF THE REGISTRY KEY
<CODE>HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINDOWS</CODE> RUN WHEN ANY USER
LOGS ON.\N\nBY DEFAULT, THE MULTISTRING <CODE>BOOTEXECUTE</CODE> VALUE OF THE REGISTRY KEY
<CODE>HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\SESSION MANAGER</CODE> IS SET TO
<CODE>AUTOCHECK AUTOCHK *</CODE>. THIS VALUE CAUSES WINDOWS, AT STARTUP, TO CHECK THE FILE-SYSTEM
INTEGRITY OF THE HARD DISKS IF THE SYSTEM HAS BEEN SHUT DOWN ABNORMALLY. ADVERSARIES CAN ADD OTHER
PROGRAMS OR PROCESSES TO THIS REGISTRY VALUE WHICH WILL AUTOMATICALLY LAUNCH AT BOOT.\N\nADVERSARIES CAN
USE THESE CONFIGURATION LOCATIONS TO EXECUTE MALWARE, SUCH AS REMOTE ACCESS TOOLS, TO MAINTAIN PERSISTENCE
THROUGH SYSTEM REBOOTS. ADVERSARIES MAY ALSO USE [MASQUERADING](HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1036)
TO MAKE THE REGISTRY ENTRIES LOOK AS IF THEY ARE ASSOCIATED WITH LEGITIMATE PROGRAMS.",
"OBJECT_MARKING_REFS": [
"MARKING-DEFINITION--FA42A846-8D90-4E51-BC29-71D5B4802168"
],
"x_MITRE_CONTRIBUTORS": [
"ODDVAR MOE, @ODDVARMOE"
],
"x_MITRE_DETECTION": "MONITOR REGISTRY FOR CHANGES TO RUN KEYS THAT DO NOT CORRELATE WITH KNOWN
SOFTWARE, PATCH CYCLES, ETC. MONITOR THE START FOLDER FOR ADDITIONS OR CHANGES. TOOLS SUCH AS SYSINTERNALS
AUTORUNS MAY ALSO BE USED TO DETECT SYSTEM CHANGES THAT COULD BE ATTEMPTS AT PERSISTENCE, INCLUDING
LISTING THE RUN KEYS' REGISTRY LOCATIONS AND STARTUP FOLDERS. (CITATION: TECHNET AUTORUNS) SUSPICIOUS
PROGRAM EXECUTION AS STARTUP PROGRAMS MAY SHOW UP AS OUTLIER PROCESSES THAT HAVE NOT BEEN SEEN BEFORE WHEN
COMPARED AGAINST HISTORICAL DATA.\N\nCHANGES TO THESE LOCATIONS TYPICALLY HAPPEN UNDER NORMAL CONDITIONS
WHEN LEGITIMATE SOFTWARE IS INSTALLED. TO INCREASE CONFIDENCE OF MALICIOUS ACTIVITY, DATA AND EVENTS
SHOULD NOT BE VIEWED IN ISOLATION, BUT AS PART OF A CHAIN OF BEHAVIOR THAT COULD LEAD TO OTHER ACTIVITIES,
SUCH AS NETWORK CONNECTIONS MADE FOR COMMAND AND CONTROL, LEARNING DETAILS ABOUT THE ENVIRONMENT THROUGH
DISCOVERY, AND LATERAL MOVEMENT.",
"CREATED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5",
```

```

"EXTERNAL_REFERENCES": [
  {
    "URL": "HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1547/001",
    "EXTERNAL_ID": "T1547.001",
    "SOURCE_NAME": "MITRE-ATTACK"
  },
  {
    "URL": "HTTPS://CAPEC.MITRE.ORG/DATA/DEFINITIONS/270.HTML",
    "EXTERNAL_ID": "CAPEC-270",
    "SOURCE_NAME": "CAPEC"
  },
  {
    "SOURCE_NAME": "MICROSOFT RUN KEY",
    "DESCRIPTION": "MICROSOFT. (N.D.). RUN AND RUNONCE REGISTRY KEYS. RETRIEVED NOVEMBER 12, 2014.",
    "URL": "HTTP://MSDN.MICROSOFT.COM/EN-US/LIBRARY/AA376977"
  },
  {
    "URL": "HTTPS://DOCS.MICROSOFT.COM/EN-US/WINDOWS/WIN32/SYSINFO/32-BIT-AND-64-BIT-APPLICATION-
DATA-IN-THE-REGISTRY",
    "DESCRIPTION": "MICROSOFT. (2018, MAY 31). 32-BIT AND 64-BIT APPLICATION DATA IN THE REGISTRY.
RETRIEVED AUGUST 3, 2020.",
    "SOURCE_NAME": "MICROSOFT WOW6432NODE 2018"
  },
  {
    "URL": "HTTPS://BLOG.MALWAREBYTES.COM/CYBERCRIME/2013/10/HIDING-IN-PLAIN-SIGHT/",
    "DESCRIPTION": "ARNTZ, P. (2016, MARCH 30). HIDING IN PLAIN SIGHT. RETRIEVED AUGUST 3, 2020.",
    "SOURCE_NAME": "MALWAREBYTES WOW6432NODE 2016"
  },
  {
    "SOURCE_NAME": "MICROSOFT RUNONCEEX APR 2018",
    "DESCRIPTION": "MICROSOFT. (2018, AUGUST 20). DESCRIPTION OF THE RUNONCEEX REGISTRY KEY.
RETRIEVED JUNE 29, 2018.",
    "URL": "HTTPS://SUPPORT.MICROSOFT.COM/HELP/310593/DESCRIPTION-OF-THE-RUNONCEEX-REGISTRY-KEY"
  },
  {
    "SOURCE_NAME": "ODDVAR MOE RUNONCEEX MAR 2018",
    "DESCRIPTION": "MOE, O. (2018, MARCH 21). PERSISTENCE USING RUNONCEEX - HIDDEN FROM
AUTORUNS.EXE. RETRIEVED JUNE 29, 2018.",
    "URL": "HTTPS://ODDVAR.MOE/2018/03/21/PERSISTENCE-USING-RUNONCEEX-HIDDEN-FROM-AUTORUNS-EXE/"
  },
  {
    "SOURCE_NAME": "TECHNET AUTORUNS",
    "DESCRIPTION": "RUSSINOVICH, M. (2016, JANUARY 4). AUTORUNS FOR WINDOWS V13.51. RETRIEVED JUNE
6, 2016.",
    "URL": "HTTPS://TECHNET.MICROSOFT.COM/EN-US/SYSINTERNALS/BB963902"
  }
],
"SPEC_VERSION": "2.1",
"X_MITRE_ATTACK_SPEC_VERSION": "2.1.0",
"X_MITRE_DOMAINS": [
  "ENTERPRISE-ATTACK"
],
"X_MITRE_MODIFIED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5"
},
{
  "TYPE": "X-DEMO-ORG-BEHAVIOR",
  "SPEC_VERSION": "2.1",
  "ID": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890DD",
  "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "SECONDARY PAYLOAD PRIVILEGE ESCALATION BEHAVIOR",
  "TACTIC": "PRIVILEGE ESCALATION",
  "TECHNIQUE": "T1134.001 - ACCESS TOKEN MANIPULATION - TOKEN IMPERSONATION",
  "FIRST_SEEN": "2022-03-31T13:00:00.000Z",
  "PLATFORMS": [
    {
      "OPERATING_SYSTEM": "MICROSOFT WINDOWS",

```

```

        "VERSION": "10"
    },
    "EXTENSIONS": {
        "EXTENSION-DEFINITION--9C59FD79-4215-4BA2-920D-3E4F320E1E62": {
            "EXTENSION_TYPE": "NEW-SDO"
        }
    },
    {
        "TYPE": "X-DEMO-ORG-DETECTION",
        "SPEC_VERSION": "2.1",
        "ID": "X-DEMO-ORG-DETECTION--F27CB358-D747-47BA-A6C4-E5B8DEBAB157",
        "CREATED": "2022-03-31T13:00:00.000Z",
        "MODIFIED": "2022-03-31T13:00:00.000Z",
        "NAME": "SECONDARY PAYLOAD PRIVILEGE ESCALATION DETECTION",
        "DATA_SOURCES": [
            {
                "DATA_TYPE": "WINEVENTLOG",
                "LOGNAME": "SECURITY",
                "EVENTCODE": "4688",
                "TASKCATEGORY": "PROCESS CREATION",
                "MESSAGE": "A NEW PROCESS HAS BEEN CREATED.\R\n\R\nCREATOR SUBJECT:\R\n\R\nTSECURITY ID:\T\TS-1-5-
21-3073171905-3635715100-2267507973-1219\R\n\R\nTACCOUNT NAME:\T\TJSMITH\R\n\R\nTACCOUNT
DOMAIN:\T\TCBIS\R\n\R\nTLOGON ID:\T\T0X502695\R\n\R\nTNTARGET SUBJECT:\R\n\R\nTSECURITY ID:\T\TS-1-5-
18\R\n\R\nTACCOUNT NAME:\T\TSP25-TARGET$\R\n\R\nTACCOUNT DOMAIN:\T\TCBIS\R\n\R\nTLOGON ID:\T\T0X3E7\R\n\R\nTPROCESS
INFORMATION:\R\n\R\nTNEW PROCESS ID:\T\T0X27584\R\n\R\nTNEW PROCESS
NAME:\TC:\Users\JSMITH.CBIS\APPDATA\LOCAL\BEACON.EXE\R\n\R\nTNTOKEN ELEVATION
TYPE:\T%1936\R\n\R\nTMANDATORY LABEL:\T\TS-1-16-16384\R\n\R\nTCREATOR PROCESS ID:\T0X26B70\R\n\R\nTCREATOR PROCESS
NAME:\TC:\Users\JSMITH\APPDATA\LOCAL\PRINTSPOOFER64.EXE\R\n\R\nTPROCESS COMMAND
LINE:\TC:\Users\JSMITH.CBIS\APPDATA\LOCAL\BEACON.EXE\R\n\R\nTNTOKEN ELEVATION TYPE INDICATES THE TYPE
OF TOKEN THAT WAS ASSIGNED TO THE NEW PROCESS IN ACCORDANCE WITH USER ACCOUNT CONTROL POLICY.\R\n\R\nTNTYPE
1 IS A FULL TOKEN WITH NO PRIVILEGES REMOVED OR GROUPS DISABLED. A FULL TOKEN IS ONLY USED IF USER
ACCOUNT CONTROL IS DISABLED OR IF THE USER IS THE BUILT-IN ADMINISTRATOR ACCOUNT OR A SERVICE
ACCOUNT.\R\n\R\nTNTYPE 2 IS AN ELEVATED TOKEN WITH NO PRIVILEGES REMOVED OR GROUPS DISABLED. AN ELEVATED
TOKEN IS USED WHEN USER ACCOUNT CONTROL IS ENABLED AND THE USER CHOOSES TO START THE PROGRAM USING RUN AS
ADMINISTRATOR. AN ELEVATED TOKEN IS ALSO USED WHEN AN APPLICATION IS CONFIGURED TO ALWAYS REQUIRE
ADMINISTRATIVE PRIVILEGE OR TO ALWAYS REQUIRE MAXIMUM PRIVILEGE, AND THE USER IS A MEMBER OF THE
ADMINISTRATORS GROUP.\R\n\R\nTNTYPE 3 IS A LIMITED TOKEN WITH ADMINISTRATIVE PRIVILEGES REMOVED AND
ADMINISTRATIVE GROUPS DISABLED. THE LIMITED TOKEN IS USED WHEN USER ACCOUNT CONTROL IS ENABLED, THE
APPLICATION DOES NOT REQUIRE ADMINISTRATIVE PRIVILEGE, AND THE USER DOES NOT CHOOSE TO START THE PROGRAM
USING RUN AS ADMINISTRATOR."
            }
        ],
        "ANALYTIC": {
            "TYPE": "SIGMA RULE",
            "RULE":
"LS0TCMF1DGHVCJ0GZGVTBWPYXRL0IAIYMDIYLZAZLZA0CMRLC2NYAXB0AW9U0IBEXRXY3RZIGXVY2FSIHVZZXIGC3BHD25PBMCGYSBWC
M9JZXNZIGFZIFNZU1RFTQPKZXRLY3RBPB246CIAGY29U2GL0AW9U0IBZZWXY3RBPB24XIGFUZCBUB3QGC2VSZWN0AW9UMGOGIHNLBGVJDGL
VBJE6CIAGICB1C2VYFGNVBNRHAW5Z0IAIJCICIKAGIEV2ZW5Q29KZTOGNDY40AOGIHNLBGVJDGLVBJI6CIAGICBZCMNFDXNLCNXJB250Y
WLUCZOGIIQICMZHBNLCG9ZAXRPMVMVZOGOGIC0GTG93CMLK0IB1C2VYDG9ZEXN0ZW1WCM9JCHJPDMMVZYWPSZXZLBD0GAGLNAAPS82DZB3V
YY2U6CIAGY2F0ZWDVNCN6IHBYS2NLC3NFZXZLBNQKICBPBMRLEDOGBWFPBGOGIHBYB2R1Y3Q6IHPBMRVD3MKC3RHDHV2OIBLHBLCLMTZ
W50YWWKDGFCNZK0KICATIGF0DGFJAY5WCML2AWXLZ2UTZXXNJYWXHDLVBGOGIC0GYXR0YWNRLQLXMTM0LJAWMQP0AXRSZTOGDXNLCIB0BYB
ZEXN0ZW0GCHJYV2VZCYBWCML2AWXLZ2UGZXNJYWXHDLVBG=="
        },
        "EXTENSIONS": {
            "EXTENSION-DEFINITION--C4690E13-107E-4796-8158-0DCF1AE7BC89": {
                "EXTENSION_TYPE": "NEW-SDO"
            }
        },
        "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894"
    },
    {
        "TYPE": "RELATIONSHIP",
        "SPEC_VERSION": "2.1",
        "ID": "RELATIONSHIP--18568EE3-837F-48D3-B807-A5F64AB3B9D8",
        "CREATED": "2022-03-31T13:00:00.000Z",
        "MODIFIED": "2022-03-31T13:00:00.000Z",

```

```

"RELATIONSHIP_TYPE": "DETECTS",
"SOURCE_REF": "X-DEMO-ORG-DETECTION--F27CB358-D747-47BA-A6C4-E5B8DEBAB157",
"TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890DD"
},
{
  "ID": "PROCESS--3BCFB0A5-BAF5-411D-B9D0-8D4B4E09BA82",
  "TYPE": "PROCESS",
  "SPEC_VERSION": "2.1",
  "IS_DEFANGED": FALSE,
  "IS_HIDDEN": FALSE,
  "PID": 0,
  "CREATED": "2022-03-31T13:00:00.000Z",
  "IMAGE_REF": "",
  "EXTENSIONS": {
    "EXTENSION-DEFINITION--F9DBE89C-0030-4A9D-8B78-0DCD0A0DE874": {
      "EXTENSION_TYPE": "PROPERTY-EXTENSION",
      "ACTION": "CREATED",
      "USER": "*$*",
      "SRC_USER": "! *$*",
      "WIN-EVENT-CODE": "4688"
    }
  }
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--A7E2AB2A-CDF5-45D0-BBE2-E6ECDB95CA99",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "USES",
  "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890DD",
  "TARGET_REF": "ATTACK-PATTERN--86850EFF-2729-40C3-B85E-C4AF26DA4A2D"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--D532F57A-908C-4CA1-8327-FCDA6D908553",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "INDICATES",
  "SOURCE_REF": "PROCESS--3BCFB0A5-BAF5-411D-B9D0-8D4B4E09BA82",
  "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890DD"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--4655B19D-C949-45BE-8316-E8861C634CAB",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "USES",
  "SOURCE_REF": "CAMPAIGN--F3BF3827-D9C5-414D-B0F0-610146FF5D85",
  "TARGET_REF": "ATTACK-PATTERN--86850EFF-2729-40C3-B85E-C4AF26DA4A2D"
},
{
  "TYPE": "ATTACK-PATTERN",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "TOKEN IMPERSONATION/THEFT",
  "X_MITRE_DATA_SOURCES": [
    "PROCESS: OS API EXECUTION",
    "COMMAND: COMMAND EXECUTION"
  ],
  "X_MITRE_VERSION": "1.0",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "X_MITRE_DEFENSE_BYPASSED": [
    "WINDOWS USER ACCOUNT CONTROL",
    "SYSTEM ACCESS CONTROLS",
    "FILE SYSTEM ACCESS CONTROLS"
  ]
},

```

```

    "X_MITRE_PLATFORMS": [
      "WINDOWS"
    ],
    "X_MITRE_IS_SUBTECHNIQUE": TRUE,
    "ID": "ATTACK-PATTERN--86850EFF-2729-40C3-B85E-C4AF26DA4A2D",
    "DESCRIPTION": "ADVERSARIES MAY DUPLICATE THEN IMPERSONATE ANOTHER USER'S TOKEN TO ESCALATE PRIVILEGES AND BYPASS ACCESS CONTROLS. AN ADVERSARY CAN CREATE A NEW ACCESS TOKEN THAT DUPLICATES AN EXISTING TOKEN USING <CODE>DUPLICATETOKEN(EX)</CODE>. THE TOKEN CAN THEN BE USED WITH <CODE>IMPERSONATELOGGEDONUSER</CODE> TO ALLOW THE CALLING THREAD TO IMPERSONATE A LOGGED ON USER'S SECURITY CONTEXT, OR WITH <CODE>SETTHREADTOKEN</CODE> TO ASSIGN THE IMPERSONATED TOKEN TO A THREAD.\N\NAN ADVERSARY MAY DO THIS WHEN THEY HAVE A SPECIFIC, EXISTING PROCESS THEY WANT TO ASSIGN THE NEW TOKEN TO. FOR EXAMPLE, THIS MAY BE USEFUL FOR WHEN THE TARGET USER HAS A NON-NETWORK LOGON SESSION ON THE SYSTEM.",
    "OBJECT_MARKING_REFS": [
      "MARKING-DEFINITION--FA42A846-8D90-4E51-BC29-71D5B4802168"
    ],
    "KILL_CHAIN_PHASES": [
      {
        "KILL_CHAIN_NAME": "MITRE-ATTACK",
        "PHASE_NAME": "DEFENSE-EVASION"
      },
      {
        "KILL_CHAIN_NAME": "MITRE-ATTACK",
        "PHASE_NAME": "PRIVILEGE-ESCALATION"
      }
    ],
    "X_MITRE_DETECTION": "IF AN ADVERSARY IS USING A STANDARD COMMAND-LINE SHELL, ANALYSTS CAN DETECT TOKEN MANIPULATION BY AUDITING COMMAND-LINE ACTIVITY. SPECIFICALLY, ANALYSTS SHOULD LOOK FOR USE OF THE <CODE>RUNAS</CODE> COMMAND. DETAILED COMMAND-LINE LOGGING IS NOT ENABLED BY DEFAULT IN WINDOWS.(CITATION: MICROSOFT COMMAND-LINE LOGGING)\N\NANALYSTS CAN ALSO MONITOR FOR USE OF WINDOWS APIS SUCH AS <CODE>DUPLICATETOKEN(EX)</CODE>, <CODE>IMPERSONATELOGGEDONUSER </CODE>, AND <CODE>SETTHREADTOKEN </CODE> AND CORRELATE ACTIVITY WITH OTHER SUSPICIOUS BEHAVIOR TO REDUCE FALSE POSITIVES THAT MAY BE DUE TO NORMAL BENIGN USE BY USERS AND ADMINISTRATORS.",
    "CREATED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5",
    "EXTERNAL_REFERENCES": [
      {
        "URL": "HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1134/001",
        "EXTERNAL_ID": "T1134.001",
        "SOURCE_NAME": "MITRE-ATTACK"
      },
      {
        "SOURCE_NAME": "MICROSOFT COMMAND-LINE LOGGING",
        "DESCRIPTION": "MATHERS, B. (2017, MARCH 7). COMMAND LINE PROCESS AUDITING. RETRIEVED APRIL 21, 2017.",
        "URL": "HTTPS://TECHNET.MICROSOFT.COM/EN-US/WINDOWS-SERVER-DOCS/IDENTITY/AD-DS/MANAGE/COMPONENT-UPDATES/COMMAND-LINE-PROCESS-AUDITING"
      }
    ],
    "SPEC_VERSION": "2.1",
    "X_MITRE_ATTACK_SPEC_VERSION": "2.1.0",
    "X_MITRE_DOMAINS": [
      "ENTERPRISE-ATTACK"
    ],
    "X_MITRE_MODIFIED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5"
  },
  {
    "TYPE": "X-DEMO-ORG-BEHAVIOR",
    "SPEC_VERSION": "2.1",
    "ID": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890EE",
    "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "NAME": "CREDENTIAL ACCESS BEHAVIOR WITH DCSYNC AND KERBEROASTING",
    "TACTIC": "CREDENTIAL ACCESS",
    "TECHNIQUE": "T1003.006 - OS CREDENTIAL DUMPING - DCSYNC",
    "FIRST_SEEN": "2022-03-31T13:00:00.000Z",
    "PLATFORMS": [
      {
        "OPERATING_SYSTEM": "MICROSOFT WINDOWS",

```



```

        "VERSION": "10"
    },
    ],
    "EXTENSIONS": {
        "EXTENSION-DEFINITION--9C59FD79-4215-4BA2-920D-3E4F320E1E62": {
            "EXTENSION_TYPE": "NEW-SDO"
        }
    },
    ],
    {
        "TYPE": "X-DEMO-ORG-DETECTION",
        "SPEC_VERSION": "2.1",
        "ID": "X-DEMO-ORG-DETECTION--275BF485-736D-4AA5-B172-E34D28FAA58C",
        "CREATED": "2022-03-31T13:00:00.000Z",
        "MODIFIED": "2022-03-31T13:00:00.000Z",
        "NAME": "DC SYNC DETECTION",
        "DATA_SOURCES": [
            {
                "DATA_TYPE": "NOTICE-TOO_SMALL",
                "LOGNAME": "/NSM/ZEEK/LOGS/CURRENT/NOTICE.LOG"
            }
        ],
    },
    "ANALYTIC": {
        "TYPE": "SIGMA RULE",
        "RULE":
        "LS0TCNRPDGXLOIBEQ1N5BMMKAQ6IGRJ3CLUYWPZDGF0DXM6IGV4CGVYAW1LBNRHBAPKZXNJCMWLDGLVB3JOGRGV0ZWN0CYBUZXR3B3JRI
        GFJDGL2AXR5IHVZAW5NIERSU0DLDE5DQ2HHBMDLCY4KDGFNZCOKICATIGF0DGFJAY5JCMVKZW50AWFSX2FJY2VZCWOIC0GYXR0YWNRLQ
        XMDAZLJAWNGPHDXROB3I6IGRLBW8KZGF0ZTOGMJAYMS8WNI8WNNWPSB2DZB3VYY2U6CIAGCHJVZHVJDDOGEMVLAOWIGLUZGV40IBTYWLUC
        IAGY2F0ZWVDCNK6IG5LDHVCMTFZXZLBNQKZGV0ZWN0AW9UOGOGIHNLBGVJDGLVB3JOKICAGIG1ZZZ0GJ2RYC3VHCGK60KRSU0DLDE5DQ2H
        HBMDLCYCK1C3JB25KAXRPB246IHNLBGVJDGLVBGPMYWXZZXBVC2L0AXZLCZOKICATIERVBWFPBIBDB250CM9SBGVYCMXLDMSOIBOAWDO"
    },
    "EXTENSIONS": {
        "EXTENSION-DEFINITION--C4690E13-107E-4796-8158-0DCF1AE7BC89": {
            "EXTENSION_TYPE": "NEW-SDO"
        }
    },
    ],
    "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894"
},
{
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--D993C3AF-9443-44DB-9478-B3A9D632D94D",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "DETECTS",
    "SOURCE_REF": "X-DEMO-ORG-DETECTION--275BF485-736D-4AA5-B172-E34D28FAA58C",
    "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890EE"
},
{
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--D4CE259F-F595-4D1D-913C-E17454396DBA",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "USES",
    "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890EE",
    "TARGET_REF": "ATTACK-PATTERN--F303A39A-6255-4B89-AECC-18C4D8CA7163"
},
{
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--CA57A603-B4D6-475E-BE8D-7618FBD58FBB",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "USES",
    "SOURCE_REF": "CAMPAIGN--F3BF3827-D9C5-414D-B0F0-610146FF5D85",
    "TARGET_REF": "ATTACK-PATTERN--F303A39A-6255-4B89-AECC-18C4D8CA7163"
},
},

```



```

{
  "OBJECT_MARKING_REFS": [
    "MARKING-DEFINITION--FA42A846-8D90-4E51-BC29-71D5B4802168"
  ],
  "TYPE": "ATTACK-PATTERN",
  "NAME": "DCSYNC",
  "X_MITRE_DATA_SOURCES": [
    "ACTIVE DIRECTORY: ACTIVE DIRECTORY OBJECT ACCESS",
    "NETWORK TRAFFIC: NETWORK TRAFFIC FLOW",
    "NETWORK TRAFFIC: NETWORK TRAFFIC CONTENT"
  ],
  "X_MITRE_VERSION": "1.0",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "KILL_CHAIN_PHASES": [
    {
      "KILL_CHAIN_NAME": "MITRE-ATTACK",
      "PHASE_NAME": "CREDENTIAL-ACCESS"
    }
  ],
  "ID": "ATTACK-PATTERN--F303A39A-6255-4B89-AECC-18C4D8CA7163",
  "X_MITRE_PLATFORMS": [
    "WINDOWS"
  ],
  "X_MITRE_IS_SUBTECHNIQUE": TRUE,
  "X_MITRE_PERMISSIONS_REQUIRED": [
    "ADMINISTRATOR"
  ],
  "DESCRIPTION": "ADVERSARIES MAY ATTEMPT TO ACCESS CREDENTIALS AND OTHER SENSITIVE INFORMATION BY ABUSING A WINDOWS DOMAIN CONTROLLER'S APPLICATION PROGRAMMING INTERFACE (API)(CITATION: MICROSOFT DRSR DEC 2017) (CITATION: MICROSOFT GETNCCCHANGES) (CITATION: SAMBA DRSUAPI) (CITATION: WINE API SAMLIB.DLL) TO SIMULATE THE REPLICATION PROCESS FROM A REMOTE DOMAIN CONTROLLER USING A TECHNIQUE CALLED DCSYNC.\N\NMEMBERS OF THE ADMINISTRATORS, DOMAIN ADMINS, AND ENTERPRISE ADMIN GROUPS OR COMPUTER ACCOUNTS ON THE DOMAIN CONTROLLER ARE ABLE TO RUN DCSYNC TO PULL PASSWORD DATA(CITATION: ADSECURITY MIMIKATZ DCSYNC) FROM ACTIVE DIRECTORY, WHICH MAY INCLUDE CURRENT AND HISTORICAL HASHES OF POTENTIALLY USEFUL ACCOUNTS SUCH AS KRBGTG AND ADMINISTRATORS. THE HASHES CAN THEN IN TURN BE USED TO CREATE A [GOLDEN TICKET](HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1558/001) FOR USE IN [PASS THE TICKET](HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1550/003)(CITATION: HARMJØY MIMIKATZ AND DCSYNC) OR CHANGE AN ACCOUNT'S PASSWORD AS NOTED IN [ACCOUNT MANIPULATION](HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1098).(CITATION: INSIDERTHREAT CHANGENTLM JULY 2017)\N\NDCSYNC FUNCTIONALITY HAS BEEN INCLUDED IN THE \"LSADUMP\" MODULE IN [MIMIKATZ](HTTPS://ATTACK.MITRE.ORG/SOFTWARE/S0002).(CITATION: GITHUB MIMIKATZ LSADUMP MODULE) LSADUMP ALSO INCLUDES NETSYN, WHICH PERFORMS DCSYNC OVER A LEGACY REPLICATION PROTOCOL.(CITATION: MICROSOFT NRPC DEC 2017)",
  "X_MITRE_CONTRIBUTORS": [
    "EXTRAHOP",
    "VINCENT LE TOUX"
  ],
  "X_MITRE_DETECTION": "MONITOR DOMAIN CONTROLLER LOGS FOR REPLICATION REQUESTS AND OTHER UNSCHEDULED ACTIVITY POSSIBLY ASSOCIATED WITH DCSYNC.(CITATION: MICROSOFT DRSR DEC 2017) (CITATION: MICROSOFT GETNCCCHANGES) (CITATION: SAMBA DRSUAPI) ALSO MONITOR FOR NETWORK PROTOCOLS(CITATION: MICROSOFT DRSR DEC 2017) (CITATION: MICROSOFT NRPC DEC 2017) AND OTHER REPLICATION REQUESTS(CITATION: MICROSOFT SAMR) FROM IPS NOT ASSOCIATED WITH KNOWN DOMAIN CONTROLLERS.(CITATION: ADSECURITY DCSYNC SEPT 2015)\N\NNOTE: DOMAIN CONTROLLERS MAY NOT LOG REPLICATION REQUESTS ORIGINATING FROM THE DEFAULT DOMAIN CONTROLLER ACCOUNT.(CITATION: HARMJØY DCSYNC SEPT 2015)",
  "CREATED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5",
  "EXTERNAL_REFERENCES": [
    {
      "URL": "HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1003/006",
      "EXTERNAL_ID": "T1003.006",
      "SOURCE_NAME": "MITRE-ATTACK"
    },
    {
      "SOURCE_NAME": "MICROSOFT DRSR DEC 2017",
      "DESCRIPTION": "MICROSOFT. (2017, DECEMBER 1). MS-DRSR DIRECTORY REPLICATION SERVICE (DRS) REMOTE PROTOCOL. RETRIEVED DECEMBER 4, 2017.",
      "URL": "HTTPS://MSDN.MICROSOFT.COM/LIBRARY/CC228086.ASPX"
    }
  ],

```

```
{
  "SOURCE_NAME": "MICROSOFT GETNCCCHANGES",
  "DESCRIPTION": "MICROSOFT. (N.D.). IDL_DRSGETNCCCHANGES (OPNUM 3). RETRIEVED DECEMBER 4, 2017.",
  "URL": "HTTPS://MSDN.MICROSOFT.COM/LIBRARY/DD207691.ASPX"
},
{
  "SOURCE_NAME": "SAMBA DRSUAPI",
  "DESCRIPTION": "SAMBAWIKI. (N.D.). DRSUAPI. RETRIEVED DECEMBER 4, 2017.",
  "URL": "HTTPS://WIKI.SAMBA.ORG/INDEX.PHP/DRSUAPI"
},
{
  "SOURCE_NAME": "WINE API SAMLIB.DLL",
  "DESCRIPTION": "WINE API. (N.D.). SAMLIB.DLL. RETRIEVED DECEMBER 4, 2017.",
  "URL": "HTTPS://SOURCE.WINEHQ.ORG/WINEAPI/SAMLIB.HTML"
},
{
  "SOURCE_NAME": "ADSECURITY MIMIKATZ DCSYNC",
  "DESCRIPTION": "METCALF, S. (2015, SEPTEMBER 25). MIMIKATZ DCSYNC USAGE, EXPLOITATION, AND
DETECTION. RETRIEVED AUGUST 7, 2017.",
  "URL": "HTTPS://ADSECURITY.ORG/?P=1729"
},
{
  "SOURCE_NAME": "HARMJ0Y MIMIKATZ AND DCSYNC",
  "DESCRIPTION": "SCHROEDER, W. (2015, SEPTEMBER 22). MIMIKATZ AND DCSYNC AND EXTRASIDS, OH MY.
RETRIEVED AUGUST 7, 2017.",
  "URL": "HTTP://WWW.HARMJ0Y.NET/BLOG/REDTEAMING/MIMIKATZ-AND-DCSYNC-AND-EXTRASIDS-OH-MY/"
},
{
  "SOURCE_NAME": "INSIDERTHREAT CHANGENTLM JULY 2017",
  "DESCRIPTION": "WARREN, J. (2017, JULY 11). MANIPULATING USER PASSWORDS WITH MIMIKATZ. RETRIEVED
DECEMBER 4, 2017.",
  "URL": "HTTPS://BLOG.STEALTHBITS.COM/MANIPULATING-USER-PASSWORDS-WITH-MIMIKATZ-SETNTLM-
CHANGENTLM"
},
{
  "SOURCE_NAME": "GITHUB MIMIKATZ LSADUMP MODULE",
  "DESCRIPTION": "DEPLY, B., LE TOUX, V. (2016, JUNE 5). MODULE ~ LSADUMP. RETRIEVED AUGUST 7,
2017.",
  "URL": "HTTPS://GITHUB.COM/GENTILKIWI/MIMIKATZ/WIKI/MODULE-~-LSADUMP"
},
{
  "SOURCE_NAME": "MICROSOFT NRPC DEC 2017",
  "DESCRIPTION": "MICROSOFT. (2017, DECEMBER 1). MS-NRPC - NETLOGON REMOTE PROTOCOL. RETRIEVED
DECEMBER 6, 2017.",
  "URL": "HTTPS://MSDN.MICROSOFT.COM/LIBRARY/CC237008.ASPX"
},
{
  "SOURCE_NAME": "MICROSOFT SAMR",
  "DESCRIPTION": "MICROSOFT. (N.D.). MS-SAMR SECURITY ACCOUNT MANAGER (SAM) REMOTE PROTOCOL
(CLIENT-TO-SERVER) - TRANSPORT. RETRIEVED DECEMBER 4, 2017.",
  "URL": "HTTPS://MSDN.MICROSOFT.COM/LIBRARY/CC245496.ASPX"
},
{
  "SOURCE_NAME": "ADSECURITY DCSYNC SEPT 2015",
  "DESCRIPTION": "METCALF, S. (2015, SEPTEMBER 25). MIMIKATZ DCSYNC USAGE, EXPLOITATION, AND
DETECTION. RETRIEVED DECEMBER 4, 2017.",
  "URL": "HTTPS://ADSECURITY.ORG/?P=1729"
},
{
  "SOURCE_NAME": "HARMJ0Y DCSYNC SEPT 2015",
  "DESCRIPTION": "SCHROEDER, W. (2015, SEPTEMBER 22). MIMIKATZ AND DCSYNC AND EXTRASIDS, OH MY.
RETRIEVED DECEMBER 4, 2017.",
  "URL": "HTTP://WWW.HARMJ0Y.NET/BLOG/REDTEAMING/MIMIKATZ-AND-DCSYNC-AND-EXTRASIDS-OH-MY/"
}
],
"SPEC_VERSION": "2.1",
"X_MITRE_ATTACK_SPEC_VERSION": "2.1.0",
"X_MITRE_DOMAINS": [
```

```

"ENTERPRISE-ATTACK"
],
"X_MITRE_MODIFIED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5"
},
{
  "TYPE": "NETWORK-TRAFFIC",
  "SPEC_VERSION": "2.1",
  "ID": "NETWORK-TRAFFIC--ACFFDF9A-BAFD-5B74-A7D9-1A6D5A4E9C5A",
  "SRC_REF": "IPV4-ADDR--57A33521-9761-54A9-81DE-3C11E441D86B",
  "DST_REF": "IPV4-ADDR--429DDAE0-A1FF-543D-99B4-F12A4A144C70",
  "PROTOCOLS": [
    "IPV4",
    "TCP",
    "HTTP",
    "HTTPS"
  ]
},
{
  "TYPE": "IPV4-ADDR",
  "SPEC_VERSION": "2.1",
  "ID": "IPV4-ADDR--429DDAE0-A1FF-543D-99B4-F12A4A144C70",
  "VALUE": "192.168.1.2"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--258248C6-6363-461A-9B8B-452D0518B2A9",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "INDICATES",
  "SOURCE_REF": "NETWORK-TRAFFIC--ACFFDF9A-BAFD-5B74-A7D9-1A6D5A4E9C5A",
  "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890EE"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--258248C6-6363-461A-9B8B-552D0518B2A9",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "INDICATES",
  "SOURCE_REF": "IPV4-ADDR--57A33521-9761-54A9-81DE-3C11E441D86B",
  "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890EE"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--258248C6-6363-461A-9B8B-652D0518B2A9",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "INDICATES",
  "SOURCE_REF": "IPV4-ADDR--429DDAE0-A1FF-543D-99B4-F12A4A144C70",
  "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890EE"
},
{
  "TYPE": "X-DEMO-ORG-BEHAVIOR",
  "SPEC_VERSION": "2.1",
  "ID": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890FF",
  "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "ABNORMAL INTERNAL NETWORK TRAFFIC FOR LATERAL MOVEMENT",
  "TACTIC": "LATERAL MOVEMENT",
  "TECHNIQUE": "T1558.001 - STEAL OR FORGE KERBEROS TICKETS - GOLDEN TICKET",
  "FIRST_SEEN": "2022-03-31T13:00:00.000Z",
  "PLATFORMS": [
    {
      "OPERATING_SYSTEM": "MICROSOFT WINDOWS",
      "VERSION": "10"
    }
  ]
}

```

```

    }
  ],
  "EXTENSIONS": {
    "EXTENSION-DEFINITION--9C59FD79-4215-4BA2-920D-3E4F320E1E62": {
      "EXTENSION_TYPE": "NEW-SDO"
    }
  }
},
{
  "TYPE": "X-DEMO-ORG-DETECTION",
  "SPEC_VERSION": "2.1",
  "ID": "X-DEMO-ORG-DETECTION--40A941CC-42DF-4B2E-B607-6D74168084B9",
  "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "LATERAL MOVEMENT DETECTION",
  "DATA_SOURCES": [
    {
      "DATA_TYPE": "WINEVENTLOG",
      "LOGNAME": "WINEVENTLOG:SECURITY"
    }
  ],
  "ANALYTIC": {
    "TYPE": "SIGMA RULE",
    "RULE":
"YXV0AG9Y0IBKZW1VCMRHDGU6IDIWMJIVMDMVMQKZGVZY3JPCHRPB246IERLDGVJDHMGCHJLLWNVNCJLBGF0ZWQGXZLBNRZIHHRH2DLZ
CBHCYBWB3RLBNRPYWWGR29SZGVUIFRPY2TLCBHDHRLBxBZCMLK0IA5MMEYMWJLZI00MTM4LTQWYJYTYTK1NS000TDIMGNLMDUXNTEKC3R
HDHVZOIBLHBLCMLTZW50YWWKDGFNZCOKICATIGF0DGFJAY5JCMVKZW50AWFSX2FJY2VZCWOIGIC0GYXR0YWNRLNQXNTU4LJAWMQPSB2DZB
3VY2U6IAOGIHB2R1Y3Q6IHDPMRVD3MKICBPBMRLD0GBWFPBGOGIGNHDGVNB3J5OIBRZXJIZXJVCWPKZXRLY3RBP246CIAGC2VSZWN
0AW9U0IAKICAGIHNVDXJJZXR5CGU6IGLUDGVYBMFSX2FSZXJ0CWOIGICAGYWLXNRFDHLWZXXJB250YWLUCZOGIKDVBGRBLRPY2TLDCKI
CBJB25KAXRPB246IHNLBGVJDGLVBGPMYWXZXBVC2L0AXZLCZOKICATIERVBWFPBIBDB250CM9SBGVYCWOGIC0GRXHJAGFUZ2UKBGV2ZWW
6IGHPZ2G="
    },
    "EXTENSIONS": {
      "EXTENSION-DEFINITION--C4690E13-107E-4796-8158-0DCF1AE7BC89": {
        "EXTENSION_TYPE": "NEW-SDO"
      }
    }
  },
  {
    "TYPE": "DOMAIN-NAME",
    "SPEC_VERSION": "2.1",
    "ID": "DOMAIN-NAME--8713B93B-186E-524D-9224-DB3B8F9FB9EF",
    "VALUE": "DATA-SERVER-DOMAIN"
  },
  {
    "TYPE": "NETWORK-TRAFFIC",
    "SPEC_VERSION": "2.1",
    "ID": "NETWORK-TRAFFIC--3564FB7D-D65C-5E02-9F55-A8A960F5C9F5",
    "SRC_REF": "IPV4-ADDR--57A33521-9761-54A9-81DE-3C11E441D86B",
    "DST_REF": "DOMAIN-NAME--8713B93B-186E-524D-9224-DB3B8F9FB9EF",
    "PROTOCOLS": [
      "IPV4"
    ]
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--19856DE6-739C-4B31-B0CC-AAA6B0B751C8",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "DETECTS",
    "SOURCE_REF": "X-DEMO-ORG-DETECTION--40A941CC-42DF-4B2E-B607-6D74168084B9",
    "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890FF"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",

```

```

    "ID": "RELATIONSHIP--476BB4F3-A9A4-4F12-AD19-52721401A673",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "INDICATES",
    "SOURCE_REF": "IPV4-ADDR--57A33521-9761-54A9-81DE-3C11E441D86B",
    "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890FF"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--476BB4F3-A9A4-4F12-AD19-52721401A673",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "INDICATES",
    "SOURCE_REF": "NETWORK-TRAFFIC--3564FB7D-D65C-5E02-9F55-A8A960F5C9F5",
    "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890FF"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--476BB4F3-A9A4-4F12-AD19-52721401A673",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "INDICATES",
    "SOURCE_REF": "DOMAIN-NAME--8713B93B-186E-524D-9224-DB3B8F9FB9EF",
    "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890FF"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--C9A2A2B3-67F3-4B8A-AD40-17C8098F7205",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "USES",
    "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890FF",
    "TARGET_REF": "ATTACK-PATTERN--7B211AC6-C815-4189-93A9-AB415DECA926"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--BAF7F0F2-1AA8-45CB-B306-CBCA8DD863D1",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "USES",
    "SOURCE_REF": "CAMPAIGN--F3BF3827-D9C5-414D-B0F0-610146FF5D85",
    "TARGET_REF": "ATTACK-PATTERN--7B211AC6-C815-4189-93A9-AB415DECA926"
  },
  {
    "OBJECT_MARKING_REFS": [
      "MARKING-DEFINITION--FA42A846-8D90-4E51-BC29-71D5B4802168"
    ],
    "TYPE": "ATTACK-PATTERN",
    "NAME": "PASS THE TICKET",
    "EXTERNAL_REFERENCES": [
      {
        "URL": "HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1550/003",
        "EXTERNAL_ID": "T1550.003",
        "SOURCE_NAME": "MITRE-ATTACK"
      },
      {
        "URL": "HTTPS://CAPEC.MITRE.ORG/DATA/DEFINITIONS/645.HTML",
        "EXTERNAL_ID": "CAPEC-645",
        "SOURCE_NAME": "CAPEC"
      },
      {
        "SOURCE_NAME": "ADSECURITY AD KERBEROS ATTACKS",
        "DESCRIPTION": "METCALF, S. (2014, NOVEMBER 22). MIMIKATZ AND ACTIVE DIRECTORY KERBEROS ATTACKS. RETRIEVED JUNE 2, 2016."
      }
    ]
  }

```

```

    "URL": "HTTPS://ADSECURITY.ORG/?P=556"
  },
  {
    "SOURCE_NAME": "GENTILKIWI PASS THE TICKET",
    "DESCRIPTION": "DEPLY, B. (2014, JANUARY 13). PASS THE TICKET. RETRIEVED JUNE 2, 2016.",
    "URL": "HTTP://BLOG.GENTILKIWI.COM/SECURITE/MIMIKATZ/PASS-THE-TICKET-KERBEROS"
  },
  {
    "SOURCE_NAME": "CAMPBELL 2014",
    "DESCRIPTION": "CAMPBELL, C. (2014). THE SECRET LIFE OF KRBTGT. RETRIEVED DECEMBER 4, 2014.",
    "URL": "HTTP://DEFCON.ORG/IMAGES/DEFCON-22/DC-22-PRESENTATIONS/CAMPBELL/DEFCON-22-CHRISTOPHER-CAMPBELL-THE-SECRET-LIFE-OF-KRBTGT.PDF"
  },
  {
    "URL": "HTTPS://STEALTHBITS.COM/BLOG/HOW-TO-DETECT-OVERPASS-THE-HASH-ATTACKS/",
    "DESCRIPTION": "WARREN, J. (2019, FEBRUARY 26). HOW TO DETECT OVERPASS-THE-HASH ATTACKS. RETRIEVED FEBRUARY 4, 2021.",
    "SOURCE_NAME": "STEALTHBITS OVERPASS-THE-HASH"
  },
  {
    "SOURCE_NAME": "CERT-EU GOLDEN TICKET PROTECTION",
    "DESCRIPTION": "ABOLINS, D., BOLDEA, C., SOCHA, K., SORIA-MACHADO, M. (2016, APRIL 26). KERBEROS GOLDEN TICKET PROTECTION. RETRIEVED JULY 13, 2017.",
    "URL": "HTTPS://CERT.EUROPA.EU/STATIC/WHITEPAPERS/UPDATED%20-%20CERT-EU_SECURITY_WHITEPAPER_2014-007_KERBEROS_GOLDEN_TICKET_PROTECTION_V1_4.PDF"
  }
],
"x_mitre_data_sources": [
  "USER ACCOUNT: USER ACCOUNT AUTHENTICATION",
  "LOGON SESSION: LOGON SESSION CREATION",
  "ACTIVE DIRECTORY: ACTIVE DIRECTORY CREDENTIAL REQUEST"
],
"x_mitre_version": "1.1",
"modified": "2022-03-31T13:00:00.000Z",
"x_mitre_system_requirements": [
  "KERBEROS AUTHENTICATION ENABLED"
],
"kill_chain_phases": [
  {
    "kill_chain_name": "MITRE-ATTACK",
    "phase_name": "DEFENSE-EVASION"
  },
  {
    "kill_chain_name": "MITRE-ATTACK",
    "phase_name": "LATERAL-MOVEMENT"
  }
],
"x_mitre_defense_bypassed": [
  "SYSTEM ACCESS CONTROLS"
],
"x_mitre_platforms": [
  "WINDOWS"
],
"x_mitre_is_subtechnique": true,
"id": "ATTACK-PATTERN--7B211AC6-C815-4189-93A9-AB415DECA926",
"description": "ADVERSARIES MAY 'PASS THE TICKET' USING STOLEN KERBEROS TICKETS TO MOVE Laterally within an environment, bypassing normal system access controls. PASS THE TICKET (PTT) is a method of authenticating to a system using Kerberos tickets without having access to an account's password. Kerberos authentication can be used as the first step to lateral movement to a remote system. When performing PTT, valid Kerberos tickets for [valid accounts](https://attack.mitre.org/techniques/T1078) are captured by [OS credential dumping](https://attack.mitre.org/techniques/T1003). A user's service tickets or ticket granting ticket (TGT) may be obtained, depending on the level of access. A service ticket allows for access to a particular resource, whereas a TGT can be used to request service tickets from the ticket granting service (TGS) to access any resource the user has privileges to access. (Citation: ADSECURITY AD Kerberos Attacks)(Citation: Gentilkiwi Pass the Ticket)\n\nA [Silver Ticket](https://attack.mitre.org/techniques/T1558/002) can be obtained for services that use Kerberos as an authentication mechanism and are used to generate tickets to access that particular resource and the system that hosts the resource (e.g., SharePoint). (Citation: ADSECURITY AD Kerberos Attacks)\n\nA [Golden

```

TICKET](HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1558/001) CAN BE OBTAINED FOR THE DOMAIN USING THE KEY DISTRIBUTION SERVICE ACCOUNT KRBtgt ACCOUNT NTLM HASH, WHICH ENABLES GENERATION OF TGTS FOR ANY ACCOUNT IN ACTIVE DIRECTORY.(CITATION: CAMPBELL 2014)\N\NADVERSARIES MAY ALSO CREATE A VALID KERBEROS TICKET USING OTHER USER INFORMATION, SUCH AS STOLEN PASSWORD HASHES OR AES KEYS. FOR EXAMPLE, \"OVERPASSING THE HASH\" INVOLVES USING A NTLM PASSWORD HASH TO AUTHENTICATE AS A USER (I.E. [PASS THE HASH](HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1550/002)) WHILE ALSO USING THE PASSWORD HASH TO CREATE A VALID KERBEROS TICKET.(CITATION: STEALTHBITS OVERPASS-THE-HASH)",

```
"X_MITRE_CONTRIBUTORS": [
  "VINCENT LE TOUX",
  "RYAN BECWAR"
],
"X_MITRE_DETECTION": "AUDIT ALL KERBEROS AUTHENTICATION AND CREDENTIAL USE EVENTS AND REVIEW FOR DISCREPANCIES. UNUSUAL REMOTE AUTHENTICATION EVENTS THAT CORRELATE WITH OTHER SUSPICIOUS ACTIVITY (SUCH AS WRITING AND EXECUTING BINARIES) MAY INDICATE MALICIOUS ACTIVITY.\N\NEVENT ID 4769 IS GENERATED ON THE DOMAIN CONTROLLER WHEN USING A GOLDEN TICKET AFTER THE KRBtgt PASSWORD HAS BEEN RESET TWICE, AS MENTIONED IN THE MITIGATION SECTION. THE STATUS CODE 0X1F INDICATES THE ACTION HAS FAILED DUE TO \"INTEGRITY CHECK ON DECRYPTED FIELD FAILED\" AND INDICATES MISUSE BY A PREVIOUSLY INVALIDATED GOLDEN TICKET.(CITATION: CERT-EU GOLDEN TICKET PROTECTION)",
"CREATED": "2022-03-31T13:00:00.000Z",
"CREATED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5",
"SPEC_VERSION": "2.1",
"X_MITRE_ATTACK_SPEC_VERSION": "2.1.0",
"X_MITRE_DOMAINS": [
  "ENTERPRISE-ATTACK"
],
"X_MITRE_MODIFIED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5"
},
{
  "TYPE": "X-DEMO-ORG-BEHAVIOR",
  "SPEC_VERSION": "2.1",
  "ID": "X-DEMO-ORG-BEHAVIOR--DE81EF18-55E6-4754-A761-6B929BF22395",
  "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "EXFILTRATION BEHAVIOR VIA BEACON",
  "TACTIC": "EXFILTRATION",
  "TECHNIQUE": "T1041 - EXFILTRATION OVER C2 CHANNEL",
  "FIRST_SEEN": "2022-03-31T13:00:00.000Z",
  "PLATFORMS": [
    {
      "OPERATING_SYSTEM": "MICROSOFT WINDOWS",
      "VERSION": "10"
    }
  ],
  "EXTENSIONS": {
    "EXTENSION-DEFINITION--9C59FD79-4215-4BA2-920D-3E4F320E1E62": {
      "EXTENSION_TYPE": "NEW-SDO"
    }
  }
},
{
  "TYPE": "X-DEMO-ORG-DETECTION",
  "SPEC_VERSION": "2.1",
  "ID": "X-DEMO-ORG-DETECTION--66AA9C25-8B56-4121-8630-DBE457393B27",
  "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "DATA EXFILTRATION DETECTION",
  "DATA_SOURCES": [
    {
      "DATA_TYPE": "ZEEK",
      "LOGNAME": [
        "/NSM/ZEEK/LOGS/CURRENT/FILES.LOG",
        "SMB"
      ]
    }
  ]
},
"ANALYTIC": {
```

```

"TYPE": "SIGMA RULE",
"RULE":
"YXV0AG9YOIBKZW1VCMRHDGU6IDIWMJIVMDMVMQKZGVZY3JPCHRPB246IERLDGVJDHMGYSBK83DUBG9HDCBMC9TIGEGC2VUC2L0AXZLI
G1VBL0B3JLZCBKAXJLY3RVCNKKAWQ6IDKYTYIXYVMMLTQXMZGTNDBINI1HOTU1LTQ5N2IYW2UWNTE1MAPZDGF0DXM6IGV4CGVYAW1LBNR
HBAP0YWDZ0GOGIC0GYXR0YWNRLMV4ZMLSDHJHDGLVBGOGIC0GYXR0YWNRLNQXMDQXCMXVZ3NVDXJJZTOGCIAGCHJVVZHVJDDOGEMVLAWOGI
GLUZGV40IBTYWLUCIAGY2F0ZWDVNCNK6IGZPBGVZCMLRDLGVJDGLVBJOKICBZZWXYL3RPB246IAOGICAGC291CMNLDHLWZTOGEMVLAWOGICA
GC291CMNLOIAVBNNLT3PLZWSVBG9NCY9JDXJYZW50L2ZPBGVZLMXVZWOGICAGZMLSZ5HBWV8Y29UDGFPBNM6ICJTZW5ZAXRPDMUGRGF0Y
SIKICBJB25KAXRPB246IHNLBGVJDGLVBGPMYXZZXBVC2L0AXZLCZOKICATIEFWCHJVDVMKIEFJY2VZC29YCWPSXZLBD0GAGLNAA=="
},
"EXTENSIONS": {
  "EXTENSION-DEFINITION--C4690E13-107E-4796-8158-0DCF1AE7BC89": {
    "EXTENSION_TYPE": "NEW-SDO"
  }
}
},
{
  "TYPE": "IPV4-ADDR",
  "SPEC_VERSION": "2.1",
  "ID": "IPV4-ADDR--3D4EE4F2-A895-5781-A0CC-B5BA466F053D",
  "VALUE": "192.168.1.3"
},
{
  "TYPE": "NETWORK-TRAFFIC",
  "SPEC_VERSION": "2.1",
  "ID": "NETWORK-TRAFFIC--FCFF628D-D69F-5D23-88B0-AEEDCFB7DA7C",
  "SRC_REF": "IPV4-ADDR--3D4EE4F2-A895-5781-A0CC-B5BA466F053D",
  "DST_REF": "IPV4-ADDR--57A33521-9761-54A9-81DE-3C11E441D86B",
  "PROTOCOLS": [
    "IPV4"
  ]
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--94AACC3-F8C4-41C0-985A-473F46312BB7",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "DETECTS",
  "SOURCE_REF": "X-DEMO-ORG-DETECTION--66AA9C25-8B56-4121-8630-DBE457393B27",
  "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--DE81EF18-55E6-4754-A761-6B929BF22395"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--476BB4F3-A9A4-4F12-AD19-52721401A673",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "INDICATES",
  "SOURCE_REF": "NETWORK-TRAFFIC--FCFF628D-D69F-5D23-88B0-AEEDCFB7DA7C",
  "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--DE81EF18-55E6-4754-A761-6B929BF22395"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--476BB4F3-A9A4-4F12-AD19-52721401A673",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "INDICATES",
  "SOURCE_REF": "IPV4-ADDR--3D4EE4F2-A895-5781-A0CC-B5BA466F053D",
  "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--DE81EF18-55E6-4754-A761-6B929BF22395"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--476BB4F3-A9A4-4F12-AD19-52721401A673",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "INDICATES",

```



```

"SOURCE_REF": "IPV4-ADDR--57A33521-9761-54A9-81DE-3C11E441D86B",
"TARGET_REF": "X-DEMO-ORG-BEHAVIOR--DE81EF18-55E6-4754-A761-6B929BF22395"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--C4E4B439-2662-47E1-B961-2B6A6FAE5241",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "USES",
  "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--DE81EF18-55E6-4754-A761-6B929BF22395",
  "TARGET_REF": "ATTACK-PATTERN--92D7DA27-2D91-488E-A00C-059DC162766D"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--FD55F673-53B0-4AE1-915B-6F30B20C950B",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "USES",
  "SOURCE_REF": "CAMPAIGN--F3BF3827-D9C5-414D-B0F0-610146FF5D85",
  "TARGET_REF": "ATTACK-PATTERN--92D7DA27-2D91-488E-A00C-059DC162766D"
},
{
  "OBJECT_MARKING_REFS": [
    "MARKING-DEFINITION--FA42A846-8D90-4E51-BC29-71D5B4802168"
  ],
  "TYPE": "ATTACK-PATTERN",
  "NAME": "EXFILTRATION OVER C2 CHANNEL",
  "EXTERNAL_REFERENCES": [
    {
      "URL": "HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1041",
      "EXTERNAL_ID": "T1041",
      "SOURCE_NAME": "MITRE-ATTACK"
    },
    {
      "SOURCE_NAME": "UNIVERSITY OF BIRMINGHAM C2",
      "DESCRIPTION": "GARDINER, J., COVA, M., NAGARAJA, S. (2014, FEBRUARY). COMMAND & CONTROL UNDERSTANDING, DENYING AND DETECTING. RETRIEVED APRIL 20, 2016.",
      "URL": "HTTPS://ARXIV.ORG/FTP/ARXIV/PAPERS/1408/1408.1136.PDF"
    }
  ],
  "X_MITRE_DATA_SOURCES": [
    "NETWORK TRAFFIC: NETWORK CONNECTION CREATION",
    "NETWORK TRAFFIC: NETWORK TRAFFIC FLOW",
    "NETWORK TRAFFIC: NETWORK TRAFFIC CONTENT",
    "FILE: FILE ACCESS",
    "COMMAND: COMMAND EXECUTION"
  ],
  "X_MITRE_VERSION": "2.1",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "KILL_CHAIN_PHASES": [
    {
      "KILL_CHAIN_NAME": "MITRE-ATTACK",
      "PHASE_NAME": "EXFILTRATION"
    }
  ],
  "X_MITRE_NETWORK_REQUIREMENTS": TRUE,
  "X_MITRE_IS_SUBTECHNIQUE": FALSE,
  "ID": "ATTACK-PATTERN--92D7DA27-2D91-488E-A00C-059DC162766D",
  "DESCRIPTION": "ADVERSARIES MAY STEAL DATA BY EXFILTRATING IT OVER AN EXISTING COMMAND AND CONTROL CHANNEL. STOLEN DATA IS ENCODED INTO THE NORMAL COMMUNICATIONS CHANNEL USING THE SAME PROTOCOL AS COMMAND AND CONTROL COMMUNICATIONS.",
  "X_MITRE_CONTRIBUTORS": [
    "WILLIAM CAIN"
  ],
},

```

"X_MITRE_DETECTION": "ANALYZE NETWORK DATA FOR UNCOMMON DATA FLOWS (E.G., A CLIENT SENDING SIGNIFICANTLY MORE DATA THAN IT RECEIVES FROM A SERVER). PROCESSES UTILIZING THE NETWORK THAT DO NOT NORMALLY HAVE NETWORK COMMUNICATION OR HAVE NEVER BEEN SEEN BEFORE ARE SUSPICIOUS. ANALYZE PACKET CONTENTS TO DETECT COMMUNICATIONS THAT DO NOT FOLLOW THE EXPECTED PROTOCOL BEHAVIOR FOR THE PORT THAT IS BEING USED. (CITATION: UNIVERSITY OF BIRMINGHAM C2)",

```
"X_MITRE_PLATFORMS": [
  "LINUX",
  "MACOS",
  "WINDOWS"
],
"CREATED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5",
"SPEC_VERSION": "2.1",
"X_MITRE_ATTACK_SPEC_VERSION": "2.1.0",
"X_MITRE_DOMAINS": [
  "ENTERPRISE-ATTACK"
],
"X_MITRE_MODIFIED_BY_REF": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5"
},
{
  "TYPE": "IDENTITY",
  "SPEC_VERSION": "2.1",
  "ID": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "DEMO"
},
{
  "OBJECT_MARKING_REFS": [
    "MARKING-DEFINITION--FA42A846-8D90-4E51-BC29-71D5B4802168"
  ],
  "TYPE": "IDENTITY",
  "ID": "IDENTITY--C78CB6E5-0C4B-4611-8297-D1B8B55E40B5",
  "IDENTITY_CLASS": "ORGANIZATION",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "NAME": "THE MITRE CORPORATION",
  "SPEC_VERSION": "2.1",
  "X_MITRE_ATTACK_SPEC_VERSION": "2.1.0",
  "X_MITRE_DOMAINS": [
    "ENTERPRISE-ATTACK"
  ],
  "X_MITRE_VERSION": "1.0"
},
{
  "TYPE": "GROUPING",
  "SPEC_VERSION": "2.1",
  "ID": "GROUPING--CB508D31-469C-41D0-AB3D-FB78ED60B61D",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "CONTEXT": "BEHAVIOR SET",
  "OBJECT_REFS": [
    "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-ED093E8279FE",
    "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AB",
    "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BC",
    "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AA",
    "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BB",
    "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890CC",
    "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890DD",
    "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890EE",
    "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890FF",
    "X-DEMO-ORG-BEHAVIOR--DE81EF18-55E6-4754-A761-6B929BF22395",
    "X-DEMO-ORG-BEHAVIOR--7F8491EF-034D-4C1A-AF9F-4B690D40793A",
    "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894"
  ]
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
```

```

    "ID": "RELATIONSHIP--98BBE11A-3AFC-4358-9B83-4AFA83F63638",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "USES",
    "SOURCE_REF": "CAMPAIGN--F3BF3827-D9C5-414D-B0F0-610146FF5D85",
    "TARGET_REF": "GROUPING--CB508D31-469C-41D0-AB3D-FB78ED60B61D"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "PART-OF",
    "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-ED093E8279FE",
    "TARGET_REF": "GROUPING--CB508D31-469C-41D0-AB3D-FB78ED60B61D"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "PART-OF",
    "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AB",
    "TARGET_REF": "GROUPING--CB508D31-469C-41D0-AB3D-FB78ED60B61D"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "PART-OF",
    "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AA",
    "TARGET_REF": "GROUPING--CB508D31-469C-41D0-AB3D-FB78ED60B61D"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "PART-OF",
    "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BB",
    "TARGET_REF": "GROUPING--CB508D31-469C-41D0-AB3D-FB78ED60B61D"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "PART-OF",
    "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890CC",
    "TARGET_REF": "GROUPING--CB508D31-469C-41D0-AB3D-FB78ED60B61D"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--B43ADC50-4CDB-4B8B-9823-0B65F074DD5F",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "PART-OF",
    "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890DD",
    "TARGET_REF": "GROUPING--CB508D31-469C-41D0-AB3D-FB78ED60B61D"
  }
}

```

```

"TYPE": "RELATIONSHIP",
"SPEC_VERSION": "2.1",
"ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
"CREATED": "2022-03-31T13:00:00.000Z",
"MODIFIED": "2022-03-31T13:00:00.000Z",
"RELATIONSHIP_TYPE": "PART-OF",
"SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890EE",
"TARGET_REF": "GROUPING--CB508D31-469C-41D0-AB3D-FB78ED60B61D"
},
{
"TYPE": "RELATIONSHIP",
"SPEC_VERSION": "2.1",
"ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
"CREATED": "2022-03-31T13:00:00.000Z",
"MODIFIED": "2022-03-31T13:00:00.000Z",
"RELATIONSHIP_TYPE": "PART-OF",
"SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890FF",
"TARGET_REF": "GROUPING--CB508D31-469C-41D0-AB3D-FB78ED60B61D"
},
{
"TYPE": "RELATIONSHIP",
"SPEC_VERSION": "2.1",
"ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
"CREATED": "2022-03-31T13:00:00.000Z",
"MODIFIED": "2022-03-31T13:00:00.000Z",
"RELATIONSHIP_TYPE": "PART-OF",
"SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--DE81EF18-55E6-4754-A761-6B929BF22395",
"TARGET_REF": "GROUPING--CB508D31-469C-41D0-AB3D-FB78ED60B61D"
},
{
"TYPE": "RELATIONSHIP",
"SPEC_VERSION": "2.1",
"ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
"CREATED": "2022-03-31T13:00:00.000Z",
"MODIFIED": "2022-03-31T13:00:00.000Z",
"RELATIONSHIP_TYPE": "PART-OF",
"SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--7F8491EF-034D-4C1A-AF9F-4B690D40793A",
"TARGET_REF": "GROUPING--CB508D31-469C-41D0-AB3D-FB78ED60B61D"
},
{
"TYPE": "RELATIONSHIP",
"SPEC_VERSION": "2.1",
"ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
"CREATED": "2022-03-31T13:00:00.000Z",
"MODIFIED": "2022-03-31T13:00:00.000Z",
"RELATIONSHIP_TYPE": "PART-OF",
"SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BC",
"TARGET_REF": "GROUPING--CB508D31-469C-41D0-AB3D-FB78ED60B61D"
},
{
"TYPE": "RELATIONSHIP",
"SPEC_VERSION": "2.1",
"ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
"CREATED": "2022-03-31T13:00:00.000Z",
"MODIFIED": "2022-03-31T13:00:00.000Z",
"RELATIONSHIP_TYPE": "OCCURS-BEFORE",
"SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BC",
"TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AA"
},
{
"TYPE": "RELATIONSHIP",
"SPEC_VERSION": "2.1",
"ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
"CREATED": "2022-03-31T13:00:00.000Z",
"MODIFIED": "2022-03-31T13:00:00.000Z",
"RELATIONSHIP_TYPE": "OCCURS-BEFORE",
"SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AB",
"TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BC"
}

```

```

    },
    {
      "TYPE": "RELATIONSHIP",
      "SPEC_VERSION": "2.1",
      "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "RELATIONSHIP_TYPE": "OCCURS-BEFORE",
      "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AA",
      "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BB"
    },
    {
      "TYPE": "RELATIONSHIP",
      "SPEC_VERSION": "2.1",
      "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "RELATIONSHIP_TYPE": "OCCURS-BEFORE",
      "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AA",
      "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890CC"
    },
    {
      "TYPE": "RELATIONSHIP",
      "SPEC_VERSION": "2.1",
      "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "RELATIONSHIP_TYPE": "OCCURS-BEFORE",
      "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BB",
      "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890DD"
    },
    {
      "TYPE": "RELATIONSHIP",
      "SPEC_VERSION": "2.1",
      "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "RELATIONSHIP_TYPE": "OCCURS-BEFORE",
      "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890DD",
      "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890EE"
    },
    {
      "TYPE": "RELATIONSHIP",
      "SPEC_VERSION": "2.1",
      "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "RELATIONSHIP_TYPE": "OCCURS-BEFORE",
      "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890EE",
      "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890FF"
    },
    {
      "TYPE": "RELATIONSHIP",
      "SPEC_VERSION": "2.1",
      "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959A4C",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "RELATIONSHIP_TYPE": "OCCURS-BEFORE",
      "SOURCE_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890FF",
      "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--DE81EF18-55E6-4754-A761-6B929BF22395"
    },
    {
      "TYPE": "EXTENSION-DEFINITION",
      "SPEC_VERSION": "2.1",
      "ID": "EXTENSION-DEFINITION--9C59FD79-4215-4BA2-920D-3E4F320E1E62",
      "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",

```

```

"NAME": "X-DEMO-ORG-BEHAVIOR EXTENSION DEFINITION",
"SCHEMA": "TBD",
"VERSION": "1.0.0",
"EXTENSION_TYPES": [
  "NEW-SDO"
]
},
{
  "TYPE": "EXTENSION-DEFINITION",
  "SPEC_VERSION": "2.1",
  "ID": "EXTENSION-DEFINITION--C4690E13-107E-4796-8158-0DCf1AE7BC89",
  "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "X-DEMO-ORG-DETECTION EXTENSION DEFINITION",
  "SCHEMA": "TBD",
  "VERSION": "1.0.0",
  "EXTENSION_TYPES": [
    "NEW-SDO"
  ]
},
{
  "TYPE": "EXTENSION-DEFINITION",
  "SPEC_VERSION": "2.1",
  "ID": "EXTENSION-DEFINITION--F9DBE89C-0030-4A9D-8B78-0DCD0A0DE874",
  "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "PROCESS EXTENSION DEFINITION",
  "SCHEMA": "TBD",
  "VERSION": "1.0.0",
  "EXTENSION_TYPES": [
    "PROPERTY-EXTENSION"
  ]
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959111",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "INDICATES",
  "SOURCE_REF": "WINDOWS-REGISTRY-KEY--C5A4244E-22D5-5797-8F78-C5FC3D1C0BDE",
  "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890CC"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959222",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "INDICATES",
  "SOURCE_REF": "PROCESS--862E625D-48BB-489E-8D4E-F7D8CD2FCAAA",
  "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AB"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959333",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "INDICATES",
  "SOURCE_REF": "PROCESS--862E625D-48BB-489E-8D4E-F7D8CD2FCBBB",
  "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AB"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",

```

```

    "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959444",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "INDICATES",
    "SOURCE_REF": "PROCESS--862E625D-48BB-489E-8D4E-F7D8CD2FCCCC",
    "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BC"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959555",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "INDICATES",
    "SOURCE_REF": "PROCESS--862E625D-48BB-489E-8D4E-F7D8CD2FCDDD",
    "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BC"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959555",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "INDICATES",
    "SOURCE_REF": "PROCESS--862E625D-48BB-489E-8D4E-F7D8CD2FCDDD",
    "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AA"
  },
  {
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959666",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "DETECTS",
    "SOURCE_REF": "X-DEMO-ORG-DETECTION--58834C29-4CEB-42A1-A218-336103021000",
    "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AA"
  },
  {
    "TYPE": "WINDOWS-REGISTRY-KEY",
    "SPEC_VERSION": "2.1",
    "ID": "WINDOWS-REGISTRY-KEY--C5A4244E-22D5-5797-8F78-C5FC3D1C0BDE",
    "KEY": "\\REGISTRY\\MACHINE\\SOFTWARE\\MICROSOFT\\WINDOWS\\CURRENTVERSION\\RUN",
    "VALUES": [
      {
        "NAME": "PERSIST"
      }
    ],
    "EXTENSIONS": {
      "EXTENSION-DEFINITION--2CF8C8C2-69F5-40F7-AA34-EFCEF2B912B1": {
        "ACTION": "MODIFY",
        "NEW_VALUE": "TRUE",
        "PROCESS_ID": "0X2498",
        "PROCESS_NAME": "C:\\WINDOWS\\REGEDIT.EXE",
        "EXTENSION_TYPE": "PROPERTY-EXTENSION"
      }
    }
  },
  {
    "ID": "PROCESS--862E625D-48BB-489E-8D4E-F7D8CD2FCAAA",
    "TYPE": "PROCESS",
    "SPEC_VERSION": "2.1",
    "IS_DEFANGED": FALSE,
    "IS_HIDDEN": FALSE,
    "PID": 0,
    "CREATED": "2022-03-31T13:00:00.000Z",
    "CWD": "",
    "COMMAND_LINE": "",
    "CREATOR_USER_REF": ""
  },

```

```

"IMAGE_REF": "",
"PARENT_REF": "",
"EXTENSIONS": {
  "EXTENSION-DEFINITION--F9DBE89C-0030-4A9D-8B78-0DCD0A0DE874": {
    "EXTENSION_TYPE": "PROPERTY-EXTENSION",
    "ACTION": "CREATED",
    "NEW-PROCESS-NAME": [
      "*OUTLOOK*",
      "THUNDERBIRD",
      "*MAIL*"
    ],
    "WIN-EVENT-CODE": "4688"
  }
}
},
{
  "ID": "PROCESS--862E625D-48BB-489E-8D4E-F7D8CD2FCBBB",
  "TYPE": "PROCESS",
  "SPEC_VERSION": "2.1",
  "IS_DEFANGED": FALSE,
  "IS_HIDDEN": FALSE,
  "PID": 0,
  "CREATED": "2022-03-31T13:00:00.000Z",
  "CWD": "",
  "COMMAND_LINE": "",
  "CREATOR_USER_REF": "",
  "IMAGE_REF": "",
  "PARENT_REF": "PROCESS--862E625D-48BB-489E-8D4E-F7D8CD2FCAAA",
  "EXTENSIONS": {
    "EXTENSION-DEFINITION--F9DBE89C-0030-4A9D-8B78-0DCD0A0DE874": {
      "EXTENSION_TYPE": "PROPERTY-EXTENSION",
      "ACTION": "CREATED",
      "CREATOR-PROCESS-NAME": [
        "*OUTLOOK*",
        "THUNDERBIRD",
        "*MAIL*"
      ],
      "NEW-PROCESS-NAME": [
        "*EDGE*",
        "*CHROME*",
        "*FIREFOX*"
      ],
      "WIN-EVENT-CODE": "4688"
    }
  }
},
{
  "ID": "PROCESS--862E625D-48BB-489E-8D4E-F7D8CD2FCCCC",
  "TYPE": "PROCESS",
  "SPEC_VERSION": "2.1",
  "IS_DEFANGED": FALSE,
  "IS_HIDDEN": FALSE,
  "PID": 0,
  "CREATED": "2022-03-31T13:00:00.000Z",
  "CWD": "",
  "COMMAND_LINE": ".*.DOCX|.PPTM|.XLSM",
  "CREATOR_USER_REF": "",
  "IMAGE_REF": "",
  "PARENT_REF": "PROCESS--862E625D-48BB-489E-8D4E-F7D8CD2FCBBB",
  "EXTENSIONS": {
    "EXTENSION-DEFINITION--F9DBE89C-0030-4A9D-8B78-0DCD0A0DE874": {
      "EXTENSION_TYPE": "PROPERTY-EXTENSION",
      "ACTION": "CREATED",
      "CREATOR-PROCESS-NAME": [
        "*EDGE*",
        "*CHROME*",
        "*FIREFOX*"
      ],
      "WIN-EVENT-CODE": "4688"
    }
  }
}

```



```

        "NEW-PROCESS-NAME": [
            "**WORD*",
            "**POWERPOINT*",
            "**EXCEL*"
        ],
        "WIN-EVENT-CODE": "4688"
    }
}
},
{
    "ID": "PROCESS--862E625D-48BB-489E-8D4E-F7D8CD2FCDDD",
    "TYPE": "PROCESS",
    "SPEC_VERSION": "2.1",
    "IS_DEFANGED": FALSE,
    "IS_HIDDEN": FALSE,
    "PID": 0,
    "CREATED": "2022-03-31T13:00:00.000Z",
    "CWD": "",
    "COMMAND_LINE": "",
    "CREATOR_USER_REF": "",
    "IMAGE_REF": "",
    "PARENT_REF": "PROCESS--862E625D-48BB-489E-8D4E-F7D8CD2FCCCC",
    "EXTENSIONS": {
        "EXTENSION-DEFINITION--F9DBE89C-0030-4A9D-8B78-0DCD0A0DE874": {
            "EXTENSION_TYPE": "PROPERTY-EXTENSION",
            "ACTION": "CREATED",
            "CREATOR-PROCESS-NAME": [
                "**WORD*",
                "**POWERPOINT*",
                "**EXCEL*"
            ],
            "NEW-PROCESS-NAME": [
                "POWERSHELL.EXE",
                "CMD.EXE"
            ],
            "WIN-EVENT-CODE": "4688"
        }
    }
},
{
    "TYPE": "X-DEMO-ORG-DETECTION",
    "SPEC_VERSION": "2.1",
    "ID": "X-DEMO-ORG-DETECTION--58834C29-4CEB-42A1-A218-336103021111",
    "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "NAME": "PROCESS 1 - SPEARPHISH",
    "DATA_SOURCES": [
        {
            "EVENTCODE": "4688",
            "LOGNAME": "SECURITY",
            "TASKCATEGORY": "PROCESS CREATION",
            "DATA_TYPE": "WINEVENTLOG:SECURITY",
            "CREATOR_PROCESS_NAME": [
                "**OUTLOOK*",
                "**THUNDERBIRD*",
                "**MAIL*"
            ],
            "NEW_PROCESS_NAME": [
                "**EDGE*",
                "**CHROME*",
                "**FIREFOX*"
            ]
        }
    ],
    "ANALYTIC": {
        "RULE":
"LS0TCNRPDGXLOIBTCGVHCNBOAXNOAW5NIHDPDGGGTGLUAWPPZDOGC3BLYXJWAGLZAGLUZWPZDGF0DXM6IGV4CGVYAW1LBNRHBAPKZXNJC

```

```
MLWDGLVB3JOGRGV0ZWN0CYBPZMZPY2UGBWFJCM8GB3BLBMLUZYBMC9TIGJYB3DZZXIUCNRHZ3M6CI0GYXR0YWNRLMLUAXRPYWXFYWNJZXN
ZCI0GYXR0YWNRLNQXNTY2LJAWMGPHDXROB3I6IGRLBW8KZGF0ZTOGMJAYMS8WNI8WNNWPSB2DZB3VYY2U6CIAGCHJZHVJDDOGD2LUZG93C
WOGIGLUZGV40IBTYWLUCIAGY2F0ZWDVNCNK6IHBYB2NLC3NFZXZLBNQKZGV0ZWN0AW9UOGOGIHNLBGVJDLVB3JOKICAGIEV2ZW50Q29KZTO
GJZQ2ODGNCIAGICBDCMVHDG9YX1BYB2NLC3NFTMFTZXXJB250YWLUCZOKICAGIC0GB3V0BG9VAW0GICAGLSB0AHVUZGVYMYLYZAOGICAGL
SBTYWLSCIAGICB0ZXFUJ3VY2VZC190YW1LFGNVBNRHAW5ZOGOGICAGLSBLZGDLCIAGICATIGNOCM9TZQOGICAGLSBMAXJLZM94CIAGY29
UZGL0AW9UOIBZWXLY3RPB24KZMFSC2VWB3NPDGL2ZXM6CI0GTG93CMXLDMMVSOIBOAWDO",
"TYPE": "SIGMA RULE - BASE64 ENCODED YAML FILE"
```

```
}
},
{
  "TYPE": "X-DEMO-ORG-DETECTION",
  "SPEC_VERSION": "2.1",
  "ID": "X-DEMO-ORG-DETECTION--58834C29-4CEB-42A1-A218-336103021222",
  "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "PROCESS 2 - SPEARPHISH",
  "DATA_SOURCES": [
    {
      "EVENTCODE": "4688",
      "LOGNAME": "SECURITY",
      "TASKCATEGORY": "PROCESS CREATION",
      "DATA_TYPE": "WINEVENTLOG:SECURITY",
      "CREATOR_PROCESS_NAME": [
        "*EDGE*",
        "*CHROME*",
        "*FIREFOX*"
      ],
      "CREATOR_COMMAND_LINE": [
        "*DOCX*",
        "*PPTM*",
        "*XLSM*"
      ],
      "NEW_PROCESS_NAME": [
        "*WORD*",
        "*POWERPOINT*",
        "*EXCEL*"
      ]
    }
  ],
  "ANALYTIC": {
    "RULE":
```

```
"LS0TCNRPDGXL0IBTCGVHNCBOAXNOAW5NIHDPDGGGTGLUAWPPZD0GC3BLYXJWAGLZAGLUZWPZDGF0DXM6IGV4CGVYAW1LBNRHBAPKZXNJC
MLWDGLVB3JOGRGV0ZWN0CYBPZMZPY2UGBWFJCM8GB3BLBMLUZYBMC9TIGJYB3DZZXIUCNRHZ3M6CI0GYXR0YWNRLMLUAXRPYWXFYWNJZXN
ZCI0GYXR0YWNRLNQXNTY2LJAWMGPHDXROB3I6IGRLBW8KZGF0ZTOGMJAYMS8WNI8WNNWPSB2DZB3VYY2U6CIAGCHJZHVJDDOGD2LUZG93C
WOGIGLUZGV40IBTYWLUCIAGY2F0ZWDVNCNK6IHBYB2NLC3NFZXZLBNQKZGV0ZWN0AW9UOGOGIHNLBGVJDLVB3JOKICAGIEV2ZW50Q29KZTO
GJZQ2ODGNCIAGICB0ZXFUJ3VY2VZC190YW1LFGNVBNRHAW5ZOGOGICAGLSB3AW53B3JKCIAGICATIGV4Y2VSCIAGICATIHBDV2VYCG9PB
NQKICAGIFBYB2NLC3NFQ29TBWUFZF9MAW5LFGNVBNRHAW5ZOGOGICAGLSBKB2NTCIAGICATIHHS20KICAGIC0GCHB0BQOGICAGQ3JLYXR
VCL9QC9JZXNZX05HBW8Y29UDGFPBNNM6CIAGICATIGVKZ2UKICAGIC0GY2HYB21LCIAGICATIGZPCMVMB3GKICB3B25KAXRPB246IHNLB
GVJDLVBGPMYWXZXBVC2L0AXZLCZOKLSBMB3CKBGV2ZW6IGHPZ2G=",
"TYPE": "SIGMA RULE - BASE64 ENCODED YAML FILE"
```

```
}
},
{
  "TYPE": "X-DEMO-ORG-DETECTION",
  "SPEC_VERSION": "2.1",
  "ID": "X-DEMO-ORG-DETECTION--58834C29-4CEB-42A1-A218-336103021000",
  "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "PROCESS - EXECUTION",
  "DATA_SOURCES": [
    {
      "EVENTCODE": "4688",
      "LOGNAME": "SECURITY",
      "TASKCATEGORY": "PROCESS CREATION",
      "DATA_TYPE": "WINEVENTLOG:SECURITY",
      "CREATOR_PROCESS_NAME": [
```

```

        "*WORD*",
        "*POWERPOINT*",
        "*EXCEL*"
    ],
    "NEW_PROCESS_NAME": [
        "/*.EXE",
        "/*.DLL"
    ]
}
],
"ANALYTIC": {
    "RULE":
"LS0TCNRPDGLXLOIBFEVJDXRPB24KAWQ6IGV4ZWN1DGLVBGPZDGF0DXM6IGV4CGVYAW1LBNRHBAPKZXNJCMWDLVB3JOGRGV0ZWN0CYBPZ
MZPY2UGBWFCJCM8GZXHLY3V0AW9UCNRHZ3M6CI0GYXR0YWNRLMV4ZWN1DGLVBGOTIGF0DGFJAY50MTA10QPHDXR0B3I6IGRLBW8KZGF0ZTO
GMJAYMS8WNI8WNWPSB2DZB3VYY2U6CIAGCHJVZHVJDDOGD2LUZG93CWOGIGLUZGV40IBTYWLUCIAGY2F0ZWDVCNK6IHBVB2NLC3NFZXZLB
NQKZGV0ZWN0AW9UOGOGIGNVBMRPDGLVB3JOGCNVUX21HY3JVIGFUZCA0BM90IGZHBHNLX3BVC2L0AXZLKQOGIHJ1BL9TYWNYBZOKICAGIEN
YZWF0B3JFUHJVY2VZC190YW1LFGNVBNRHAWSZOGOGICAGLSB3B3JKCIAGICATIHBDV2VYCG9PBNQKICAGIC0GZXHJZWKKICAGIE5LD19QC
M9JZXNZX05HBWV8ZW5KC3DPDGG6CIAGICATICIUZXHLIGOGICAGLSAILMRSBCKICAGIEV2ZW50Q29KZT0GJZQ20DGNCIAGZMFSC2VFCG9
ZAXRPMU6CIAGICBOZXFUJHVY2VZC190YW1LFGNVBNRHAWSZOGOGICAGLSBZCGX3B3C2NAPMYWXZXBVC2L0AXZLZCOKLSBMB3CKBGV2Z
WW6IGHPZ2G=",
    "TYPE": "SIGMA RULE - BASE64 ENCODED YAML FILE"
}
},
{
    "TYPE": "X-DEMO-ORG-DETECTION",
    "SPEC_VERSION": "2.1",
    "ID": "X-DEMO-ORG-DETECTION--458C02C9-3635-42E4-8873-6785E00517E7",
    "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "NAME": "REGISTRY - PERSISTENCE",
    "DATA_SOURCES": [
        {
            "EVENTCODE": "4657",
            "LOGNAME": "SECURITY",
            "MESSAGE": "A REGISTRY VALUE WAS MODIFIED.\N\NSUBJECT:\N\TSECURITY ID:\T\TS-1-5-21-1102256457-
2379380313-1247321256-500\N\TACCOUNT NAME:\T\TADMINISTRATOR\N\TACCOUNT DOMAIN:\T\TSP17\N\TLOGON
ID:\T\T0X1A1ADFEB\N\N\TOBJECT
NAME:\T\T\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\N\TOBJECT VALUE
NAME:\TPERSIST\N\THANDLE ID:\T\T0X918\N\TOPERATION TYPE:\T\TNEW REGISTRY VALUE CREATED\N\NPROCESS
INFORMATION:\N\TPROCESS ID:\T\T0X18F0\N\TPROCESS
NAME:\T\TC:\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE\N\NCHANGE INFORMATION:\N\TOLD
VALUE TYPE:\T\T-\N\TOLD VALUE:\T\T-\N\TNEW VALUE TYPE:\T\TREG_SZ\N\TNEW VALUE:\T\TTTRUE",
            "TASKCATEGORY": "REGISTRY",
            "DATA_TYPE": "WINEVENTLOG:SECURITY"
        }
    ],
    "ANALYTIC": {
        "RULE":
"LS0TCNRPDGLXLOIBSZWDPC3RYESBSDW4GS2V5CWPPZDOGCMVAXN0CNKGCGVYC2LZDGVUY2UKC3RHDHVZ0IBLHBLCMLTZW50YWWKZGVZY
3JPCRHPB246IERLDGVJDHMGMBMV3IHJLZ2LZDHJ5IHJ1BIBRXKGY3JLYXRLZCBLDMVUDC4KDGFNZOKLSBHDHRY2SUCGVYC2LZDGVUY2U
KLSBHDHRY2SUDE1NDCKYXV0AG9YOIBKZW1VCMRHDGU6IDIWMJEVMDYVMDCKBG9NC291CMNLOGOGIHBVB2R1Y3Q6IHDPMRVD3MKICBPB
MRLEDGBWFBPGOGIGNHDGVNB3J50IBYZWDPC3RYEV9LDMVUDAPKXRLY3RBPB246CIAGC2VSZWN0AW9UOGOGICAGRXZLBNRDB2RLOIANNDY
1NYCKICAGIE9IAMVJDF90YW1LFGNVBNRHAWSZOGOGICAGLSBDSW4KICAGIC0GU2HLBGWGRM9SZGVYCWOGIGNVBMRPDGLVB3JOGC2VSZWN0A
W9UCMZHBHNLG9ZAXRPMVMZOGOTIEHPZ2GKBGV2ZWW6IGHPZ2G=",
        "TYPE": "SIGMA RULE - BASE64 ENCODED YAML FILE"
    }
}
},
{
    "TYPE": "RELATIONSHIP",
    "SPEC_VERSION": "2.1",
    "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959666",
    "CREATED": "2022-03-31T13:00:00.000Z",
    "MODIFIED": "2022-03-31T13:00:00.000Z",
    "RELATIONSHIP_TYPE": "DETECTS",
    "SOURCE_REF": "X-DEMO-ORG-DETECTION--58834C29-4CEB-42A1-A218-336103021111",
    "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890AB"
}
},

```

```
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959666",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "DETECTS",
  "SOURCE_REF": "X-DEMO-ORG-DETECTION--58834C29-4CEB-42A1-A218-336103021222",
  "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890BC"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-914343959666",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "DETECTS",
  "SOURCE_REF": "X-DEMO-ORG-DETECTION--458C02C9-3635-42E4-8873-6785E00517E7",
  "TARGET_REF": "X-DEMO-ORG-BEHAVIOR--EDC99806-F8E9-4EE3-B2D4-1234567890CC"
},
{
  "TYPE": "X-DEMO-ORG-DETECTION-GROUP",
  "SPEC_VERSION": "2.1",
  "ID": "X-DEMO-ORG-DETECTION-GROUP--58834C29-4CEB-42A1-A218-321103021999",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "NAME": "REAPER LITE DETECTION",
  "DESCRIPTION": "THIS DETECTION GROUP DETECTS SPEARPHISHING, EXECUTION, AND PERSISTENCE",
  "CORRELATION_WORKFLOWS": [
    {
      "TYPE": "CACAO WORKFLOW",
      "NOTE": "PLACEHOLDER FOR CORRELATION IN CACAO STANDARD",
      "WORKFLOW": "TBD"
    },
    {
      "TYPE": "BPMN - BASE64 ENCODED .BPMN (XML) FILE",
      "NOTE": "DECODE BASE64 STRING AND SAVE AS .BPMN FILE",
      "WORKFLOW":
"PD94BWWGDMVYC2LVBj0TMS4WIIbLBMNVZGLUZZ0IVVRGLTGIPZ4KPGJWBW46ZGVMAW5PDGLVBNMGEG1SBNM6YNBtBJ0IAHR0CDOVL3D3D
Y5VBWCUB3JNL3NWZWMVQLBNTI8YMDewMDUyNC9NT0RFTCIGEG1SBNM6YNBtBMRPPSJODHRW0I8VD3D3LM9TZYSVCMVC3BLY99CUE10LZI
WMTAWNTI0L0RJIIb4BWXUCZPKYZ0IAHR0CDOVL3D3DY5VBWCUB3JNL3NWZWMVREQVMJAXMDA1MJQVREMIHHTBG5ZOMRPPSJODHRW0I8VD
3D3LM9TZYSVCMVC3BLY99ERC8YMDewMDUyNC9ESSIGEG1SBNM6YMLVYZ0IAHR0CDOVL2JWBW4UAW8VC2N0ZW1HL2JWBW4VYMLVY29SB3I
VMS4WIIb4BWXUCZPJb2XVCJ0IAHR0CDOVL3D3DY5VBWCUB3JNL3NWZWMVQLBNTI9UB24TBM9YBWF0AXZLL2NVBG9YLZEUMCIGAWQ9IKRLZ
MLUAXRPB25XZFSBDDMBX0IiHRCMDLDE5HBWVZCGFJZT0IAHR0CDOVL2JWBW4UAW8VC2N0ZW1HL2JWBW4IIGV4CG9YDGVYPSJDYw11BMR
HIE1VZGVSXZIIIGV4CG9YDGVYVMVYC2LVBj0INC4XMI4WIj4KICA8YNBtBJPWCm9JZNXZIGLKPSJQCM9JZNXZXFxBMVDNGOIIGLZXHLY
3V0YWJSZT0IDHJ1ZSI+CtAGICA8YNBtBJPZDGFYDEV2Zw50XZIEIG5HbWU9IK9MZMLJZSBNYWNyBYbTCGVHCNB
OAXNOIDEGQWXLcNQIPGOGICAGICA8YNBtBJPVDXRNb2LUZZ5GBG93XZE3ANJUN308L2JWBW46B3V0Z29PBMC+CIAGICAGIDXCIG1UONNPZ
25HBEV2Zw50RGVMAW5PDGLVbIPZD0IU2LNBmFSRXZLBNREZWPBML0AW9UXZF3ZWJ0BHAIIC8+CIAGICA8L2JWBW46C3RHCNRFDMVUDD4
KICAGIDXCIG1UONN0YXJ0RXZLBNQGAWQ9IKV2Zw50XZE0NH2EMOIIG5HbWU9IK9MZMLJZSBNYWNyBYbFEGVJDXRPB24GQWXLcNQIPGOGI
CAGICA8YNBtBJPVDXRNb2LUZZ5GBG93XZB6NTIwZMK8L2JWBW46B3V0Z29PBMC+CIAGICAGIDXCIG1UONNPZ25HBEV2Zw50RGVMAW5PDGL
VBIPZD0IU2LNBmFSRXZLBNREZWPBML0AW9UXZFVNXJUCYXIIC8+CIAGICA8L2JWBW46C3RHCNRFDMVUDD4KICAGIDXCIG1UONN0YXJ0R
XZLBNQGAWQ9IKV2Zw50XEZMHFSDDIIG5HbWU9IK9MZMLJZSBNYWNyBYbTCGVHCNB0AXNOIDIGQWXLcNQIPGOGICAGICA8YNBtBJPVDX
RNb2LUZZ5GBG93XZFRN210AHA8L2JWBW46B3V0Z29PBMC+CIAGICAGIDXCIG1UONNPZ25HBEV2Zw50RGVMAW5PDGLVbIPZD0IU2LNBmFS
RXZLBNREZWPBML0AW9UXZB1DHR0MJMIIC8+CIAGICA8L2JWBW46C3RHCNRFDMVUDD4KICAGIDXCIG1UONN0YXJ0RXZLBNQGAWQ9IKV2Zw5
0XZFWCDHRZ3IIG5HbWU9ILJLZ2LZDHJ5IE1VZCB8BGVYDCI+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMTN3ZNMWODWVYNBtBJPVD
XRNb2LUZZ4KICAGICAGPGJWBW46C2LNBmFSRXZLBNREZWPBML0AW9UIGLKPSJTAWduYXWFDmVUDERLZMLUAXRPB25FMXB5DG5QBSIGLZ4
KICAGIDWVYNBtBJPZDGFYDEV2Zw50PGOGICAGPGJWBW46C3RHCNRFDMVUDCBPZD0IRXZLBNRFMGXHDMM5MSIGBMFTZT0IRENTEW5JIEFSZ
XJ0IJ4KICAGICAGPGJWBW46B3V0Z29PBMC+RMXVD18XBGS1DJb4PC9ICG1UOM91DGDVAW5NPGOGICAGICA8YNBtBJPZAWduYXWFDmVUDER
LZMLUAXRPB24GAWQ9LNP225HBEV2Zw50RGVMAW5PDGLVbL8WBGZAZM0IiAVPogGICAGPC9ICG1UONN0YXJ0RXZLBNQ+CIAGICA8YNBtB
JPZDGFYDEV2Zw50IGLKPSJFDMVUDF8XCJD50HY4IIBUYw1LPsJFEGZPBCBBBGVYDCI+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMGR
SOXLICJWVYNBtBJPVDXRNb2LUZZ4KICAGICAGPGJWBW46C2LNBmFSRXZLBNREZWPBML0AW9UIGLKPSJTAWduYXWFDmVUDERLZMLUAXRPB
25FMHJL0WDXYZYJGLZ4KICAGIDWVYNBtBJPZDGFYDEV2Zw50PGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZE3ANJUN30IiHN
VDXJZZVJLZJ0IU3RHCNRFDMVUDF8XIIB0YXJNZXR5Zwy9IKFJDGL2AXR5XZB00XBOY20IIC8+CIAGICA8YNBtBJP0YXNRIGLKPSJB3YRPD
ML0EV8WDDLWAGNTIIBUYw1LPsJDB2XSZWN0ICHUAW1LLCBIB3N0LCBQCM9JZNXZIELEKSBMB3IGV2VIIIEJYB3DZZXIGY2F5BGVKIGZYB20
GRW1HAWWIPGOGICAGICA8YNBtBJPPBMNBWBLUZZ5GBG93XZE3ANJUN308L2JWBW46AW5JB21PBMC+CIAGICAGIDXCIG1UOM91DGDVAW5NP
KZSB3DFMGJ2A3VRMZWVYNBtBJPVDXRNb2LUZZ4KICAGIDWVYNBtBJP0YXNRPGOGICAGPGJWBW46D6DGFZAYBPZD0IQNW0AXZPDHLFMH0YZK
ZNYIGBMFTZT0IUXVLcNKGYWDHAW5ZDCBtCGVHCNB0AXNOIDIGQWXLcNRZIJ4KICAGICAGPGJWBW46AW5JB21PBMC+RMXVD18WYNZRDWSZP
C9ICG1UOMLUY29TAW5NPGOGICAGICA8YNBtBJPVDXRNb2LUZZ5GBG93XZEWOdbSEWk8L2JWBW46B3V0Z29PBMC+CIAGICA8L2JWBW46DGF
```



ZAZK4KICAGIDXCIG1UONNLXCVLBMNLRMXVDYBPZD0IRMXVD18WYNZRDSW5IIBZB3VYV2VSZWY9IKFJDGL2AXR5XZB0OXBOY20IIRHCHMDLDFJLZJ0IQWN0AXZPDHLMFHMB0YKZNYTGLZ4KICAGIDXCIG1UONRHC2SGAWQ9IKFJDGL2AXR5XZFXZHNYCIVIG5HBWU9IKNVBGXLY3QGKFRPBWUSIEHVC3QSIFBYB2NLC3MGSURZKSBCMKM9TIGJYB3DZXXIGB3BLBMLUZYBTVWYNYBYBK2BMPGOGICAGICA8YNTBJPJPBMNVBLWLUZZ5GBG93XZFRN210AHA812JBWB463W5J21PBM+C+IAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMH0VADBQDDWVYNTBJ3PVDXRN2LUZZ4KICAGIDWVYNTBJP0YXNRPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZFRN210AHAIHNVDXJ3JZVJLZJ0IRXZLBNRFMTMWCXW0MSIGDGFY2ZV0UMVMP5JBY3RPDML0EV8XCWRZC2J2I1AVPGOGICAGPGJWBW46C2XHBVZAXZLR2F0ZXDHESBPZD0IR2F0ZXDH0V8XN2ZMC3HLIIBUYW1LPSJCYB0AGVY2S5BHBIFB6WFPBCB0BYBXZWI9W5KIFDLIIB0BYBPZMGYP2UGYWN0AXPDHKB24GAG9ZDCBPBIBZAG9YDCB0A1U1LZNJBHWU/1J4KICAGICAGPGJWBW46W5J21PBM+C+RMXVD18XNGDWBHLPPC9ICG1UOMLUY29TAW5NPGOGICAGICA8YNTBJ3PBMNVBLWLUZZ5GBG93XZB00HGEZENQ8L2JBWB46W5J21PBM+C+IAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMXZPEW82NJWVYNTBJ3PVDXRN2LUZZ4KICAGICAGPGJWBW46B3V0Z29PBM+C+RMXVD18XCN3MGR0PC9ICG1UOM91DGDVAW5NPGOGICAGPG9ICG1UOMV4Y2X1C2L2ZUDHDGV3YXK+C+IAGICA8YNTBJ3PZZXF1ZW5JZUSB3CGAWQ9IKZSB3DFMT4AMG5AS1GC291CNMLUMVMP5JBY3RPDML0EV8WCHRCJOTM3IIB0YXJNZKRSZ9YIKDHDG6V3YXLFMTDMZNN4ZS1GLZ4KICAGIDXCIG1UOMVUEZV2W50TGLKPSJFDMVUDF8WJAH4ZHYIIBUYW1LPSJTDG9W1J4KICAGICGPGJWBW46W5J21PBM+C+RMXVD18XMDL5BZY2PC9ICG1UOMLUY29TAW5NPGOGICAGPG9ICG1UOMVUEZV2W50TGLKPSJFDMVUDF8WJAH4ZHYIIBUYW1LPSJTDG9W1J4KICAGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZ2AXLVNJYIIG5HBWU9IK5PIIBZB3VYV2VSZWY9IKDHDGV3YXLFMTDMZNN4ZS1GIDGFY2ZV0UMVMP5JFDMVUDF8WJAH4ZHYIIBUYW1LPSJTDG9W1J4KICAGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZ2AXLVNJYIIG5HBWU9IK5PIIBZB3VYV2VSZWY9IKDHDGV3YXLFMTDMZNN4ZS1GIDGFY2ZV0UMVMP5JFDMVUDF8WJAH4ZHYIIBUYW1LPSJTDG9W1J4KICAGICAGPGJWBW46B3V0Z29PBM+C+RMXVD18XNGZNTDPC9ICG1UOM91DGDVAW5NPGOGICAGPG9ICG1UONBHCMF5BG9V2F0ZXDHET4KICAGIDXCIG1UONRHC2SGAWQ9IKFJDGL2AXR5XZBQ0DYXBM0IIG5HBWU9ILF1XZJ5IGFNWYUUC3QGU3BLXYXWAGLZACAXIEF5XZJ0CYI+C+IAGICAGIDXCIG1UOMLUY29TAW5NPKZSB3DFMXJ3BHPWADWVYNTBJ3PBMNVBLWLUZZ4KICAGICAGPGJWBW46B3V0Z29PBM+C+RMXVD18WADH4M3P0C9ICG1UOM91DGDVAW5NPGOGICAGPG9ICG1UONRHC2S+C+IAGICA8YNTBJ3PZZXF1ZW5JZUZS3CGAWQ9IKZSB3DFMXJ3BHPWACIG291CNMLUMVMP5JHYXRLD2F5XZFMZJRCDQIIRHCHMDLDFJLZJ0IQWN0AXZPDHLMF0G4NJ3FUBSIGLZ4KICAGIDXCIG1UONNLXCVLBMNLRMXVDYBPZD0IRMXVD18WADH4M3P0IIBZB3VYV2VSZWY9IKFJDGL2AXR5XZBQ0DYXBM0IIRHCHMDLDFJLZJ0IR2F0ZXDH0V8XN2ZMC3HLI1IIVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZFYDTCWZGJIG5HBWU9ILLFUYIGC291CNMLUMVMP5JHYXRLD2F5XZ3ZMZZE6GUTIIHRCMDLDFJLZJ0IQWN0AXZPDHLMF0G4NJ3FUBSIGLZ4KICAGIDXCIG1UONNLXCVLBMNLRMXVDYBPZD0IRMXVD18WADH4M3P0IIBZB3VYV2VSZWY9IKFJDGL2AXR5XZBQ0DYXBM0IIRHCHMDLDFJLZJ0IR2F0ZXDH0V8XN2ZMC3HLI1IIVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZFYDTCWZGJIG5HBWU9ILLFUYIGC291CNMLUMVMP5JHYXRLD2F5XZ3ZMZZE6GUTIIHRCMDLDFJLZJ0IQWN0AXZPDHLMF0G4NJ3FUBSIGLZ4KICAGIDXCIG1UONNLXCVLBMNLRMXVDYBPZD0IRMXVD18WADH4M3P0IIBZB3VYV2VSZWY9IKFJDGL2AXR5XZBQ0DYXBM0IIRHCHMDLDFJLZJ0IR2F0ZXDH0V8XN2ZMC3HLI1IIVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZFYDTCWZGJIG5HBWU9ILLFUYIGC291CNMLUMVMP5JHYXRLD2F5XZ3ZMZZE6GUTIIHRCMDLDFJLZJ0IQWN0AXZPDHLMF0G4NJ3FUBSIGLZ4KICAGIDXCIG1UONNLXCVLBMNLRMXVDYBPZD0IRMXVD18WADH4M3P0IIBZB3VYV2VSZWY9IKFJDGL2AXR5XZBQ0DYXBM0IIRHCHMDLDFJLZJ0IR2F0ZXDH0V8XN2ZMC3HLI1IIVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZFYDTCWZGJIG5HBWU9ILLFUYIGC291CNMLUMVMP5JHYXRLD2F5XZ3ZMZZE6GUTIIHRCMDLDFJLZJ0IQWN0AXZPDHLMF0G4NJ3FUBSIGLZ4KICAGIDXCIG1UONNLXCVLBMNLRMXVDYBPZD0IRMXVD18WADH4M3P0IIBZB3VYV2VSZWY9IKFJDGL2AXR5XZBQ0DYXBM0IIRHCHMDLDFJLZJ0IR2F0ZXDH0V8XN2ZMC3HLI1IIVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZFYDTCWZGJIG5HBWU9ILLFUYIGC291CNMLUMVMP5JHYXRLD2F5XZ3ZMZZE6GUTIIHRCMDLDFJLZJ0IQWN0AXZPDHLMF0G4NJ3FUBSIGLZ4KICAGIDXCIG1UONNLXCVLBMNLRMXVDYBPZD0IRMXVD18WADH4M3P0IIBZB3VYV2VSZWY9IKFJDGL2AXR5XZBQ0DYXBM0IIRHCHMDLDFJLZJ0IR2F0ZXDH0V8XN2ZMC3HLI1IIVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZFYDTCWZGJIG5HBWU9ILLFUYIGC291CNMLUMVMP5JHYXRLD2F5XZ3ZMZZE6GUTIIHRCMDLDFJLZJ0IQWN0AXZPDHLMF0G4NJ3FUBSIGLZ4KICAGIDXCIG1UONNLXCVLBMNLRMXVDYBPZD0IRMXVD18WADH4M3P0IIBZB3VYV2VSZWY9IKFJDGL2AXR5XZBQ0DYXBM0IIRHCHMDLDFJLZJ0IR2F0ZXDH0V8XN2ZMC3HLI1IIVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZFYDTCWZGJIG5HBWU9ILLFUYIGC291CNMLUMVMP5JHYXRLD2F5XZ3ZMZZE6GUTIIHRCMDLDFJLZJ0IQWN0AXZPDHLMF0G4NJ3FUBSIGLZ4KICAGIDXCIG1UONNLXCVLBMNLRMXVDYBPZD0IRMXVD18WADH4M3P0IIBZB3VYV2VSZWY9IKFJDGL2AXR5XZBQ0DYXBM0IIRHCHMDLDFJLZJ0IR2F0ZXDH0V8XN2ZMC3HLI1IIVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZFYDTCWZGJIG5HBWU9ILLFUYIGC291CNMLUMVMP5JHYXRLD2F5XZ3ZMZZE6GUTIIHRCMDLDFJLZJ0IQWN0AXZPDHLMF0G4NJ3FUBSIGLZ4KICAGIDXCIG1UONNLXCVLBMNLRMXVDYBPZD0IRMXVD18WADH4M3P0IIBZB3VYV2VSZWY9IKFJDGL2AXR5XZBQ0DYXBM0IIRHCHMDLDFJLZJ0IR2F0ZXDH0V8XN2ZMC3HLI1IIVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZFYDTCWZGJIG5HBWU9ILLFUYIGC291CNMLUMVMP5JHYXRLD2F5XZ3ZMZZE6GUTIIHRCMDLDFJLZJ0IQWN0AXZPDHLMF0G4NJ3FUBSIGLZ4KICAGIDXCIG1UONNLXCVLBMNLRMXVDYBPZD0IRMXVD18WADH4M3P0IIBZB3VYV2VSZWY9IKFJDGL2AXR5XZBQ0DYXBM0IIRHCHMDLDFJLZJ0IR2F0ZXDH0V8XN2ZMC3HLI1IIVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZFYDTCWZGJIG5HBWU9ILLFUYIGC291CNMLUMVMP5JHYXRLD2F5XZ3ZMZZE6GUTIIHRCMDLDFJLZJ0IQWN0AXZPDHLMF0G4NJ3FUBSIGLZ4KICAGIDXCIG1UONNLXCVLBMNLRMXVDYBPZD0IRMXVD18WADH4M3P0IIBZB3VYV2VSZWY9IKFJDGL2AXR5XZBQ0DYXBM0IIRHCHMDLDFJLZJ0IR2F0ZXDH0V8XN2ZMC3HLI1IIVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZFYDTCWZGJIG5HBWU9ILLFUYIGC291CNMLUMVMP5JHYXRLD2F5XZ3ZMZZE6GUTIIHRCMDLDFJLZJ0IQWN0AXZPDHLMF0G4NJ3FUBSIGLZ4KICAGIDXCIG1UONNLXCVLBMNLRMXVDYBPZD0IRMXVD18WADH4M3P0IIBZB3VYV2VSZWY9IKFJDGL2AXR5XZBQ0DYXBM0IIRHCHMDLDFJLZJ0IR2F0ZXDH0V8XN2ZMC3HLI1IIVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZFYDTCWZGJIG5HBWU9ILLFUYIGC291CNMLUMVMP5JHYXRLD2F5XZ3ZMZZE6GUTIIHRCMDLDFJLZJ0IQWN0AXZPDHLMF0G4NJ3FUBSIGLZ4KICAGIDXCIG1UONNLXCVLBMNLRMXVDYBPZD0IRMXVD18WADH4M3P0IIBZB3VYV2VSZWY9IKF

MPSJHYXRLD2F5XZFUAWH0YJGIIHRHCDLDFJLZJ0IQWN0AXZPDHLMFTJLA29XDSIGLZ4KICAGIDXCIG1UONRHC2SGAWQ9IKFJDGL2AXR5X
ZB0XAWDTMIIG5HBWU9ILF1XZJ5IGFNYWLC3QGUMVNAAXN0CNKGTW9KIEF5XZJ0I4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XNMJE
50GTLPC9ICG1UOMLUY29TAW5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZE5M2V5BHC8L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWB
W46DGFZAZ4KICAGIDXCIG1UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18WNRDVMNJNIIBZB3VYV2V5ZWY9IKFJDGL2AXR5XZEY2WTVCXUIIHR
HCDLDFJLZJ0IR2F0ZXDHEV8WZNNUYMOXIIVAPGOGICAGPGJWBW46DGFZAYBPZD0IQWN0AXZPDHLMFG9TNXUXZCIGBMFTZT0IQ29SBGVJD
CBUAW1LLCBIB3N0LCBQSUQSIE5LD19WYWX1ZSI+CIAGICAGIDXCIG1UOMLUY29TAW5NPKZSB3DFMTN3ZNMWODWVYNTBJPPBMNVBWLZZ4
KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18XANZ5CWSIPCG1UOM91DGDVAW5NPGOGICAGPC9ICG1UONRHC2S+CIAGICA8YNTBTPZZ
XF1Z5JZUZSB3CGAWQ9IKZSB3DFMTN3ZNMWOCIGC291CMNLUMVMPSJFDMVUDF8XCHA4A2DYIIB0YXJNZXRSZWY9IKFJDGL2AXR5XZBVBTV
1M0QIIC8+CIAGICA8YNTBTPZZXF1Z5JZUZSB3CGAWQ9IKZSB3DFMWP2EXFUYIIGC291CMNLUMVMPSJBY3RPDML0EV8WB201DTFKIIB0Y
XJNZXRSZWY9IKFJDGL2AXR5XZEWCWZ4CJMIIC8+CIAGICA8YNTBTPZZXJ2AWNLVGFZAYBPZD0IQWN0AXZPDHLMFTBXZNHYMYIGBMFTZT0
IU2VHCMN0IGZVCIBQSUQGDGHDCB3CMVHDGVKIHROAXMGCHJYV2VZCYI+CIAGICAGIDXCIG1UOMLUY29TAW5NPKZSB3DFMWP2EXFUYJWVY
NBTBJPPBMNVBWLZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18WOG5SZHVRPC9ICG1UOM91DGDVAW5NPGOGICAGPC9ICG1UONNLCNZ
PY2VUYXNRPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZA4BMXKDW5IHNVDXJJZVJLZJ0IQWN0AXZPDHLMFTBXZNHYMYIGD
GFY2Z0UMVMPSJHYXRLD2F5XZB1YMXWD2UIC8+CIAGICA8YNTBTPWYXJHGBGLBEDHDGV3YXKGAWQ9IKDHDGV3YXLFMHVIBHB3ZSI+CIA
GICAGIDXCIG1UOMLUY29TAW5NPKZSB3DFMDHUBGR1AZWVYNTBTPPBMNVBWLZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18XDJDL
NLP9C9ICG1UOM91DGDVAW5NPGOGICAGPC9ICG1UONBCHMFSBGVS2F0ZXDHET4KICAGIDXCIG1UONRHC2SGAWQ9IKFJDGL2AXR5XZF1NXL
LEG0IIG5HBWU9ILF1XZJ5IEFNYWLC3QGTWJCM8GRXHL3V0AW9UIEF5XZJ0I4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XDJDL
NLP9C9ICG1UOMLUY29TAW5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZBHMWLC308L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWBW4
6DGFZAZ4KICAGIDXCIG1UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18XDJDLMLPIIBZB3VYV2V5ZWY9IKDHDGV3YXLFMHVIBHB3ZSIGDGFY
2V0UMVMPSJBY3RPDML0EV8XYJV0ZXHTIIVAPGOGICAGPGJWBW46XZHXJBHVAXZLR2F0ZXDHEBSPZD0IR2F0ZXDHEV8XNW8ZNGM5IIBUYW1
LPSJEAQWQDGBCFWEUGB3IGREXMIHNWYXDIUEGEG3JYV2VGB0AWDTMIGI1VCGRLZC8S2WDP3CYET8IPGOGICAGICA8YNTBTPPBMNVB
WLZZ5GBG93XZE5M2V5BHC8L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOMLUY29TAW5NPKZSB3DFMGEXAW9ZEJWVYNTBTPPBMNVBWL
UZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18XCDRMMJKYPC9ICG1UOM91DGDVAW5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93X
ZFXD2LRDM8L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWBW46XZHXJBHVAXZLR2F0ZXDHET4KICAGIDXCIG1UONNLCXVBLMNLRMXVDYBPZD0
IRMXVD18XOTNLWEX3IIBZB3VYV2V5ZWY9IKFJDGL2AXR5XZB0XAWDTMIIHRHCDLDFJLZJ0IR2F0ZXDHEV8XNW8ZNGM5IIVAPGOGICAGP
GJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZBHMWLC30IHNVDXJJZVJLZJ0IQWN0AXZPDHLMWI1DGV4BSIGDGFY2V0UMVMPSJHYXR
LD2F5XZE1BZM0YKZIKC8+CIAGICA8YNTBTP0YXNRIGLKPSJBY3RPDML0EV8XA2M5YWF0IIBUYW1LPSJ5ZWNVCMQGTWJCM8GC3BHD25LZ
CBWCM9JZXNZIHR0YXQGBW9KZGVKIFJLZYAOQWRKIDEGCG9PBNQPIJ4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XCDRMMJKYPC9ICG1
UOMLUY29TAW5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZFMOWRSM08L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWBW46DGFZAZ4KIC
AGIDXCIG1UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18XCDRMMJKYIIBUYW1LPSJZXXMIHNVDXJJZVJLZJ0IR2F0ZXDHEV8XNW8ZNGM5IIB
0YXJNZXRSZWY9IKFJDGL2AXR5XZFRY2LHYWGIC8+CIAGICA8YNTBTPZZXF1Z5JZUZSB3CGAWQ9IKZSB3DFMTIX0THRZSIGC291CMNL
UMVMPSJHYXRLD2F5XZBMC25IAJIEIHRHCDLDFJLZJ0IQWN0AXZPDHLMHQ5CDB1MYIGLZ4KICAGIDXCIG1UONBCHMFSBGVS2F0ZXDHEB
PZD0IR2F0ZXDHEV8WZNNUYMOXIIVAPGOGICAGPGJWBW46AW5JB21PBMCM+RMXVD18WNRDVMNJPNC9ICG1UOMLUY29TAW5NPGOGICAGICA8Y
NBTBJPVDXRN2LUZZ5GBG93XZEYMTK4A2U8L2JWBW46B3V0Z29PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMWM0XCNJWJWVYNT
BTPVDXRN2LUZZ4KICAGIDWVYNTBTPWYXJHGBGLBEDHDGV3YXK+CIAGICA8YNTBTPJLBMRFDMVUDCBPZD0IRXZLBNRFRMWRUBW10DSIGB
MFTZT0U3RVCCI+CIAGICAGIDXCIG1UOMLUY29TAW5NPKZSB3DFMFX3AWT2YZWVYNTBTPPBMNVBWLZZ4KICAGIDWVYNTBTPJLBMRFDMV
UDD4KICAGIDXCIG1UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18XCDPA3ZJIIIBUYW1LPSJ0BYIGC291CMNLUMVMPSJHYXRLD2F5XZE1BZM0Y
ZKIIHRHCDLDFJLZJ0IRXZLBNRFRMWRUBW10DSIGLZ4KICAGIDXCIG1UONN0YXJ0RXZLBNQGAWQ9IKV2Z5W0XZA0ZWH6YW8IIG5HBWU9IKJ
LYWNBKF5XZJ0I4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18XBNW0AWQ3PC9ICG1UOM91DGDVAW5NPGOGICAGICA8YNTBTPJZAWDUY
WXFDMVUDERLZMLUAXRPB24GAWQ9ILNPZ25HBEV2Z5W0RGVMAW5PDGLVBL8WDWQ2Z3BYIIIVAPGOGICAGPC9ICG1UONN0YXJ0RXZLBNQ+CIA
GICA8YNTBTPZDGFYDEV2Z5W0IGLKPSJFDMVUDF8XOXLRZDB3IIBUYW1LPSJQCM2LRXNJIEFSZXJ0I4KICAGICAGPGJWBW46B3V0Z29P
MC+RMXVD18XCDJ20HNIP9C9ICG1UOM91DGDVAW5NPGOGICAGICA8YNTBTPJZAWDUYWXFDMVUDERLZMLUAXRPB24GAWQ9ILNPZ25HBEV2Z5
0RGVMAW5PDGLVBL8XBNWJZBWKXIIIVAPGOGICAGPC9ICG1UONN0YXJ0RXZLBNQ+CIAGICA8YNTBTP0YXNRIGLKPSJBY3RPDML0EV8XZLITC
3BKIIIBUYW1LPSJDB2XSZN0IFRPBWUSIEHVC3QSIHRVA2VUIGLUZM8SIGFJY291BNQGAW5MBYI+CIAGICAGIDXCIG1UOMLUY29TAW5NPKZ
SB3DFMAYD0JHYJWVYNTBTPPBMNVBWLZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18XBTQYCW5ZPC9ICG1UOM91DGDVAW5NPGOGI
CAGPC9ICG1UONRHC2S+CIAGICA8YNTBTPZZXF1Z5JZUZSB3CGAWQ9IKZSB3DFMAYD0JHYIIGC291CMNLUMVMPSJFDMVUDF8XOXLRZDB
3IIB0YXJNZXRSZWY9IKFJDGL2AXR5XZF20W1ZCGQIIC8+CIAGICA8YNTBTPZZXF1Z5JZUZSB3CGAWQ9IKZSB3DFMWM0MNFUCYIGC291C
MNLUMVMPSJBY3RPDML0EV8XZJLTC3BKIIIBUYW1JNZXRSZWY9IKDHDGV3YXLFMDEQCDRMCISGLZ4KICAGIDXCIG1UONBCHMFSBGVS2F0ZXD
HESBPZD0IR2F0ZXDHEV8WMTWNGZIXJ4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XBTQYCW5ZPC9ICG1UOMLUY29TAW5NPGOGICAGI
CA8YNTBTPVDXRN2LUZZ5GBG93XZFWCZFZOW88L2JWBW46B3V0Z29PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMGJQD282DJW
VYNTBTPVDXRN2LUZZ4KICAGIDWVYNTBTPWYXJHGBGLBEDHDGV3YXK+CIAGICA8YNTBTPZZXF1Z5JZUZSB3CGAWQ9IKZSB3DFMFXBZM
XMSBYIGC291CMNLUMVMPSJHYXRLD2F5XZAXNHA0ZNEIHRHCDLDFJLZJ0IQWN0AXZPDHLMGLMMZFYIYGLZ4KICAGIDXCIG1UONNLCNZ
PY2VUYXNRIGLKPSJBY3RPDML0EV8WAWYMXJJIIIBUYW1LPSJDCMVDHVGUGY2FZZS9UB3RPDMLJYXRPB24DGD8GAW52ZXN0AWDHDGUGUJPD
IBFC2MIPGOGICAGICA8YNTBTPPBMNVBWLZZ5GBG93XZFWCZFZOW88L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZ
SB3DFMHLVN3GXMJWVYNTBTPVDXRN2LUZZ4KICAGIDWVYNTBTPZZXJ2AWNLVGFZAZ4KICAGIDXCIG1UOMV4Y2X1C2L2ZUDHDGV3YXKGA
WQ9IKDHDGV3YXLFMHQ5ZMM3BSIGBMFTZT0IV2FZIFBAXYGRXNJIGZB20GT9UL5VCM1HBCBBY3RPDML0ET8IPGOGICAGICA8YNTBTP
PBMNVBWLZZ5GBG93XZB5ZDQMTI8L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMFXU1ZGVVWCZWVYNTBTPVD
XRN2LUZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18WEWNSANC0PC9ICG1UOM91DGDVAW5NPGOGICAGPC9ICG1UOMV4Y2X1C2L2ZUD
HDGV3YXK+CIAGICA8YNTBTPZZXF1Z5JZUZSB3CGAWQ9IKZSB3DFMHLVN3GXMIGC291CMNLUMVMPSJBY3RPDML0EV8WAWYMXJJIIIB0Y
XJNZXRSZWY9IKDHDGV3YXLFMHQ5ZMM3BSIGLZ4KICAGIDXCIG1UONRHC2SGAWQ9IKFJDGL2AXR5XZB1MXWCTYIIG5HBWU9ILJLY29Y2CB
BYMSVCM1HBCB8Y2IEVZYAAQWRKIDEGUG9PBNQPIJ4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XDTVKZBZPC9ICG1UOMLUY29TAW
5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZFDTLFBI8L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWBW46DGFZAZ4KICAGIDXCIG1
UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18XDTVKZXBZIIIBUYW1LPSJZXXMIHNVDXJJZVJLZJ0IR2F0ZXDHEV8WDDLMY2DTIIB0YXJNZXRSZ
WY9IKFJDGL2AXR5XZB1MXWCTYIIC8+CIAGICA8YNTBTPJLBMRFDMVUDCBPZD0IRXZLBNRFRMDB1CDI2MYIGBMFTZT0IU3RVCCI+CIAGICA
GIDXCIG1UOMLUY29TAW5NPKZSB3DFMHLJBGPN3DWVYNTBTPPBMNVBWLZZ4KICAGIDWVYNTBTPJLBMRFDMVUDD4KICAGIDXCIG1UONNLC
XVBLMNLRMXVDYBPZD0IRMXVD18WEWNSANC0IIBUYW1LPSJ0BYIGC291CMNLUMVMPSJHYXRLD2F5XZAXNHA0ZNEIHRHCDLDFJLZJ0IQWN0AXZPDHLMGLMMZFYIYGLZ4KICAGIDXCIG1UONNLCNZ
PY2VUYXNRIGLKPSJBY3RPDML0EV8WAWYMXJJIIIBUYW1LPSJDCMVDHVGUGY2FZZS9UB3RPDMLJYXRPB24DGD8GAW52ZXN0AWDHDGUGUJPD
IBFC2MIPGOGICAGICA8YNTBTPPBMNVBWLZZ5GBG93XZFWCZFZOW88L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZ
SB3DFMHLVN3GXMJWVYNTBTPVDXRN2LUZZ4KICAGIDWVYNTBTPZZXJ2AWNLVGFZAZ4KICAGIDXCIG1UOMV4Y2X1C2L2ZUDHDGV3YXKGA
WQ9IKDHDGV3YXLFMHQ5ZMM3BSIGBMFTZT0IV2FZIFBAXYGRXNJIGZB20GT9UL5VCM1HBCBBY3RPDML0ET8IPGOGICAGICA8YNTBTP
PBMNVBWLZZ5GBG93XZB5ZDQMTI8L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMFXU1ZGVVWCZWVYNTBTPVD
XRN2LUZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18WEWNSANC0PC9ICG1UOM91DGDVAW5NPGOGICAGPC9ICG1UOMV4Y2X1C2L2ZUD
HDGV3YXK+CIAGICA8YNTBTPZZXF1Z5JZUZSB3CGAWQ9IKZSB3DFMHLVN3GXMIGC291CMNLUMVMPSJBY3RPDML0EV8WAWYMXJJIIIB0Y
XJNZXRSZWY9IKDHDGV3YXLFMHQ5ZMM3BSIGLZ4KICAGIDXCIG1UONRHC2SGAWQ9IKFJDGL2AXR5XZB1MXWCTYIIG5HBWU9ILJLY29Y2CB
BYMSVCM1HBCB8Y2IEVZYAAQWRKIDEGUG9PBNQPIJ4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XDTVKZBZPC9ICG1UOMLUY29TAW
5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZFDTLFBI8L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWBW46DGFZAZ4KICAGIDXCIG1
UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18XDTVKZXBZIIIBUYW1LPSJZXXMIHNVDXJJZVJLZJ0IR2F0ZXDHEV8WDDLMY2DTIIB0YXJNZXRSZ
WY9IKFJDGL2AXR5XZB1MXWCTYIIC8+CIAGICA8YNTBTPJLBMRFDMVUDCBPZD0IRXZLBNRFRMDB1CDI2MYIGBMFTZT0IU3RVCCI+CIAGICA
GIDXCIG1UOMLUY29TAW5NPKZSB3DFMHLJBGPN3DWVYNTBTPPBMNVBWLZZ4KICAGIDWVYNTBTPJLBMRFDMVUDD4KICAGIDXCIG1UONNLC
XVBLMNLRMXVDYBPZD0IRMXVD18WEWNSANC0IIBUYW1LPSJ0BYIGC291CMNLUMVMPSJHYXRLD2F5XZAXNHA0ZNEIHRHCDLDFJLZJ0IQWN0AXZPDHLMGLMMZFYIYGLZ4KICAGIDXCIG1UONNLCNZ
PY2VUYXNRIGLKPSJBY3RPDML0EV8WAWYMXJJIIIBUYW1LPSJDCMVDHVGUGY2FZZS9UB3RPDMLJYXRPB24DGD8GAW52ZXN0AWDHDGUGUJPD
IBFC2MIPGOGICAGICA8YNTBTPPBMNVBWLZZ5GBG93XZFWCZFZOW88L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZ
SB3DFMHLVN3GXMJWVYNTBTPVDXRN2LUZZ4KICAGIDWVYNTBTPZZXJ2AWNLVGFZAZ4KICAGIDXCIG1UOMV4Y2X1C2L2ZUDHDGV3YXKGA
WQ9IKDHDGV3YXLFMHQ5ZMM3BSIGBMFTZT0IV2FZIFBAXYGRXNJIGZB20GT9UL5VCM1HBCBBY3RPDML0ET8IPGOGICAGICA8YNTBTP
PBMNVBWLZZ5GBG93XZB5ZDQMTI8L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMFXU1ZGVVWCZWVYNTBTPVD
XRN2LUZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18WEWNSANC0PC9ICG1UOM91DGDVAW5NPGOGICAGPC9ICG1UOMV4Y2X1C2L2ZUD
HDGV3YXK+CIAGICA8YNTBTPZZXF1Z5JZUZSB3CGAWQ9IKZSB3DFMHLVN3GXMIGC291CMNLUMVMPSJBY3RPDML0EV8WAWYMXJJIIIB0Y
XJNZXRSZWY9IKDHDGV3YXLFMHQ5ZMM3BSIGLZ4KICAGIDXCIG1UONRHC2SGAWQ9IKFJDGL2AXR5XZB1MXWCTYIIG5HBWU9ILJLY29Y2CB
BYMSVCM1HBCB8Y2IEVZYAAQWRKIDEGUG9PBNQPIJ4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XDTVKZBZPC9ICG1UOMLUY29TAW
5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZFDTLFBI8L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWBW46DGFZAZ4KICAGIDXCIG1
UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18XDTVKZXBZIIIBUYW1LPSJZXXMIHNVDXJJZVJLZJ0IR2F0ZXDHEV8WDDLMY2DTIIB0YXJNZXRSZ
WY9IKFJDGL2AXR5XZB1MXWCTYIIC8+CIAGICA8YNTBTPJLBMRFDMVUDCBPZD0IRXZLBNRFRMDB1CDI2MYIGBMFTZT0IU3RVCCI+CIAGICA
GIDXCIG1UOMLUY29TAW5NPKZSB3DFMHLJBGPN3DWVYNTBTPPBMNVBWLZZ4KICAGIDWVYNTBTPJLBMRFDMVUDD4KICAGIDXCIG1UONNLC
XVBLMNLRMXVDYBPZD0IRMXVD18WEWNSANC0IIBUYW1LPSJ0BYIGC291CMNLUMVMPSJHYXRLD2F5XZAXNHA0ZNEIHRHCDLDFJLZJ0IQWN0AXZPDHLMGLMMZFYIYGLZ4KICAGIDXCIG1UONNLCNZ
PY2VUYXNRIGLKPSJBY3RPDML0EV8WAWYMXJJIIIBUYW1LPSJDCMVDHVGUGY2FZZS9UB3RPDMLJYXRPB24DGD8GAW52ZXN0AWDHDGUGUJPD
IBFC2MIPGOGICAGICA8YNTBTPPBMNVBWLZZ5GBG93XZFWCZFZOW88L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZ
SB3DFMHLVN3GXMJWVYNTBTPVDXRN2LUZZ4KICAGIDWVYNTBTPZZXJ2AWNLVGFZAZ4KICAGIDXCIG1UOMV4Y2X1C2L2ZUDHDGV3YXKGA
WQ9IKDHDGV3YXLFMHQ5ZMM3BSIGBMFTZT0IV2FZIFBAXYGRXNJIGZB20GT9UL5VCM1HBCBBY3RPDML0ET8IPGOGICAGICA8YNTBTP
PBMNVBWLZZ5GBG93XZB5ZDQMTI8L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMFXU1ZGVVWCZWVYNTBTPVD
XRN2LUZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18WEWNSANC0PC9ICG1UOM91DGDVAW5NPGOGICAGPC9ICG1UOMV4Y2X1C2L2ZUD
HDGV3YXK+CIAGICA8YNTBTPZZXF1Z5JZUZSB3CGAWQ9IKZSB3DFMHLVN3GXMIGC291CMNLUMVMPSJBY3RPDML0EV8WAWYMXJJIIIB0Y
XJNZXRSZWY9IKDHDGV3YXLFMHQ5ZMM3BSIGLZ4KICAGIDXCIG1UONRHC2SGAWQ9IKFJDGL2AXR5XZB1MXWCTYIIG5HBWU9ILJLY29Y2CB
BYMSVCM1HBCB8Y2IEVZYAAQWRKIDEGUG9PBNQPIJ4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XDTVKZBZPC9ICG1UOMLUY29TAW
5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZFDTLFBI8L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWBW46DGFZAZ4KICAGIDXCIG1
UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18XDTVKZXBZIIIBUYW1LPSJZXXMIHNVDXJJZVJLZJ0IR2F0ZXDHEV8WDDLMY2DTIIB0YXJNZXRSZ
WY9IKFJDGL2AXR5XZB1MXWCTYIIC8+CIAGICA8YNTBTPJLBMRFDMVUDCBPZD0IRXZLBNRFRMDB1CDI2MYIGBMFTZT0IU3RVCCI+CIAGICA
GIDXCIG1UOMLUY29TAW5NPKZSB3DFMHLJBGPN3DWVYNTBTPPBMNVBWLZZ4KICAGIDWVYNTBTPJLBMRFDMVUDD4KICAGIDXCIG1UONNLC
XVBLMNLRMXVDYBPZD0IRMXVD18WEWNSANC0IIBUYW1LPSJ0BYIGC291CMNLUMVMPSJHYXRLD2F5XZAXNHA0ZNEIHRHCDLDFJLZJ0IQWN0AXZPDHLMGLMMZFYIYGLZ4KICAGIDXCIG1UONNLCNZ
PY2VUYXNRIGLKPSJBY3RPDML0EV8WAWYMXJJIIIBUYW1LPSJDCMVDHVGUGY2FZZS9UB3RPDMLJYXRPB24DGD8GAW52ZXN0AWDHDGUGUJPD
IBFC2MIPGOGICAGICA8YNTBTPPBMNVBWLZZ5GBG93XZFWCZFZOW88L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZ
SB3DFMHLVN3GXMJWVYNTBTPVDXRN2LUZZ4KICAGIDWVYNTBTPZZXJ2AWNLVGFZAZ4KICAGIDXCIG1UOMV4Y2X1C2L2ZUDHDGV3YXKGA
WQ9IKDHDGV3YXLFMHQ5ZMM3BSIGBMFTZT0IV2FZIFBAXYGRXNJIGZB20GT9UL5VCM1HBCBBY3RPDML0ET8IPGOGICAGICA8YNTBTP
PBMNVBWLZZ5GBG93XZB5ZDQMTI8L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMFXU1ZGVVWCZWVYNTBTPVD
XRN2LUZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18WEWNSANC0PC9ICG1UOM91DGDVAW5NPGOGICAGPC9ICG1UOMV4Y2X1C2L2ZUD
HDGV3YXK+CIAGICA8YNTBTPZZXF1Z5JZUZSB3CGAWQ9IKZSB3DFMHLVN3GXMIGC291CMNLUMVMPSJBY3RPDML0EV8WAWYMXJJIIIB0Y
XJNZXRSZWY9IKDHDGV3YXLFMHQ5ZMM3BSIGLZ4KICAGIDXCIG1UONRHC2SGAWQ9IKFJDGL2AXR5XZB1MXWCTYIIG5HBWU9ILJLY29Y2CB
BYMSVCM1HBCB8Y2IEVZYAAQWRKIDEGUG9PBNQPIJ4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XDTVKZBZPC9ICG1UOMLUY29TAW
5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZFDTLFBI8L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWBW46DGFZAZ4KICAGIDXCIG1
UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18XDTVKZXBZIIIBUYW1LPSJZXXMIHNVDXJJZVJLZJ0IR2F0ZXDHEV8WDDLMY2DTIIB0YXJNZXRSZ
WY9IKFJDGL2AXR5XZB1MXWCTYIIC8+CIAGICA8YNTBTPJLBMRFDMVUDCBPZD0IRXZLBNRFRMDB1CDI2MYIGBMFTZT0IU3RVCCI+CIAGICA
GIDXCIG1UOMLUY29TAW5NPKZSB3DFMHLJBGPN3DWVYNTBTPPBMNVBWLZZ4KICAGIDWVYNTBTPJLBMRFDMVUDD4KICAGIDXCIG1UONNLC
XVBLMNLRMXVDYBPZD0IRMXVD18WEWNSANC0IIBUYW1LPSJ0BYIGC291CMNLUMVMPSJHYXRLD2F5XZAXNHA0ZNEIHRHCDLDFJLZJ0IQWN0AXZPDHLMGLMMZFYIYGLZ4KICAGIDXCIG1UONNLCNZ
PY2VUYXNRIGLKPSJBY3RPDML0EV8WAWYMXJJIIIBUYW1LPSJDCMVDHVGUGY2FZZS9UB3RPDMLJYXRPB24DGD8GAW52ZXN0AWDHDGUGUJPD
IBFC2MIPGOGICAGICA8YNTBTPPBMNVBWLZZ5GBG93XZFWCZFZOW88L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZ
SB3DFMHLVN3GXMJWVYNTBTPVDXRN2LUZZ4KICAGIDWVYNTBTPZZXJ2AWNLVGFZAZ4KICAGIDXCIG1UOMV4Y2X1C2L2ZUDHDGV3YXKGA
WQ9IKDHDGV3YXLFMHQ5ZMM3BSIGBMFTZT0IV2FZIFBAXYGRXNJIGZB20GT9UL5VCM1HBCBBY3RPDML0ET8IPGOGICAGICA8YNTBTP
PBMNVBWLZZ5GBG93XZB5ZDQMTI8L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMFXU1ZGVVWCZWVYNTBTPVD
XRN2LUZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18WEWNSANC0PC9ICG1UOM91DGDVAW5NPGOGICAGPC9ICG1UOMV4Y2X1C2L2ZUD
HDGV3YXK+CIAGICA8YNTBTPZZXF1Z5JZUZSB3CGAWQ9IKZSB3DFMHLVN3GXMIGC291CMNLUMVMPSJBY3RPDML0EV8WAWYMXJJIIIB0Y
XJNZXRSZWY9IKDHDGV3YXLFMHQ5ZMM3BSIGLZ4KICAGIDXCIG1UONRHC2SGAWQ9IKFJDGL2AXR5XZB1MXWCTYIIG5HBWU9ILJLY29Y2CB
BYMSVCM1HBCB8Y2IEVZYAAQWRKIDEGUG9PBNQPIJ4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XDTVKZBZPC9ICG1UOMLUY29TAW
5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZFDTLFBI8L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWBW46DGFZAZ4KICAGIDXCIG1
UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18XDTVKZXBZIIIBUYW1LPSJZXXMIHNVDXJJZVJLZJ0IR2F0ZXDHEV8WDDLMY2DTIIB0YXJNZXRSZ
WY9IKFJDGL2AXR5XZB1MXWCTYIIC8+CIAGICA8YNTBTPJLBMRFDMVUDCBPZD0IRXZLBNRFRMDB1CDI2MYIGBMFTZT0IU3RVCCI+CIAGICA
GIDXCIG1UOMLUY29TAW5NPKZSB3DFMHLJBGPN3DWVYNTBTPPBMNVBWLZZ4KICAGIDWVYNTBTPJLBMRFDMVUDD4KICAGIDXCIG1UONNLC
XVBLMNLRMXVDYBPZD0IRMXVD18WEWNSANC0IIBUYW1LPSJ0BYIGC291CMNLUMVMPSJHYXRLD2F5XZAXNHA0ZNEIHRHCDLDFJLZJ0IQWN0AXZPDHLMGLMMZFYIYGLZ4KICAGIDXCIG1UONNLCNZ
PY2VUYXNRIGLKPSJBY3RPDML0EV8WAWYMXJJIIIBUYW1LPSJDCMVDHVGUGY2FZZS9UB3RPDMLJYXRPB24DGD8GAW52ZXN0AWDHDGUGUJPD
IBFC2MIPGOGICAGICA8YNTBTPPBMNVBWLZZ5GBG93XZFWCZFZOW88L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZ
SB3DFMHLVN3GXMJWVYNTBTPVDXRN2LUZZ4KICAGIDWVYNTBTPZZXJ2AWNLVGFZAZ4KICAGIDXCIG1UOMV4Y2X1C2L2ZUDHDGV3YXKGA
WQ9IKDHDGV3YXLFMHQ5ZMM3BSIGBMFTZT0IV2FZIFBAXYGRXNJIGZB20GT9UL5VCM1HBCBBY3RPDML0ET8IPGOGICAGICA8YNTBTP
PBMNVBWLZZ5GBG93XZB5ZDQMTI8L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMFXU1ZGVVWCZWVYNTBTPVD
XRN2LUZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18WEWNSANC0PC9ICG1UOM91DGDVAW5NPGOGICAGPC9ICG1UOMV4Y2X1C2L2ZUD
HDGV3YXK+CIAGICA8YNTBTPZZXF1Z5JZUZSB3CGAWQ9IKZSB3DFMHLVN3GXMIGC291CMNLUMVMPSJBY3RPDML0EV8WAWYMXJJIIIB0Y
XJNZXRSZWY9IKDHDGV3YXLFMHQ5ZMM3BSIGLZ4KICAGIDXCIG1UONRHC2SGAWQ9IKFJDGL2AXR5XZB1MXWCTYIIG5HBWU9ILJLY29Y2CB
BYMSVCM1HBCB8Y2IEVZYAAQWRKIDEGUG9PBNQPIJ4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XDTVKZBZPC9ICG1UOMLUY29TAW
5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZFDTLFBI8L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWBW46DGFZAZ4KICAGIDXCIG1
UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18XDTVKZXBZIIIBUYW1LPSJZXXMIHNVDXJJZVJLZJ0IR2F0ZXDHEV8WDDLMY2DTIIB0YXJNZXRSZ
WY9IKFJDGL2AXR5XZB1MXWCTYIIC8+CIAGICA8YNTBTPJLBMRFDMVUDCBPZD0IRXZLBNRFRMDB1CDI2MYIGBMFTZT0IU3RVCCI+CIAGICA
GIDXCIG1UOMLUY29TAW5NPKZSB3DFMHLJBGPN3DWVYNTBTPPBMNVBWLZZ4KICAGIDWVYNTBTPJLBMRFDMVUDD4KICAGIDXCIG1UONNLC
XVBLMNLRMXVDYBPZD0IRMXVD18WEWNSANC0IIBUYW1LPSJ0BYIGC291CMNLUMVMPSJHYXRLD2F5XZAXNHA0ZNEIHRHCDLDFJLZJ0IQWN0AXZPDHLMGLMMZFYIYGLZ4KICAGIDXCIG1UONNLCNZ
PY2VUYXNRIGLKPSJBY3RPDML0EV8WAWYMXJJIIIBUYW1LPSJDCMVDHVGUGY2FZZS9UB3RPDMLJYXRPB24DGD8GAW52ZXN0AWDHDGUGUJPD
IBFC2MIPGOGICAGICA8YNTBTPPBMNVBWLZZ5GBG93XZFWCZFZOW88L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZ
SB3DFMHLVN3GXMJWVYNTBTPVDXRN2LUZZ4KICAGIDWVYNTBTPZZXJ2AWNLVGFZAZ4KICAGIDXCIG1UOMV4Y2X1C2L2ZUDHDGV3YXKGA
WQ9IKDHDGV3YXLFMHQ5ZMM3BSIGBMFTZT0IV2FZIFBAXYGRXNJIGZB20GT9UL5VCM1HBCBBY3RPDML0ET8IPGOGICAGICA8YNTBTP
PBMNVBWLZZ5GBG93XZB5ZDQMTI8L2JWBW46AW5JB21PBMCM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMFXU1ZGVVWCZWVYNTBTPVD
XRN2LUZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18WEWNSANC0PC9ICG1UOM91DGDVAW5NPGOGICAGPC9ICG1UOMV4Y2X1C2L2ZUD
HDGV3YXK+CIAGICA8YNTBTPZZXF1Z5JZUZSB3CGAWQ9IKZSB3DFMHLVN3GXMIGC291CMNLUMVMPSJBY3RPDML0EV8WAWYMXJJIIIB0Y
XJNZXRSZWY9IKDHDGV3YXLFMHQ5ZMM3BSIGLZ4KICAGIDXCIG1UONRHC2SGAWQ9IKFJDGL2AXR5XZB1MXWCTYIIG5HBWU9ILJLY29Y2CB
BYMSVCM1HBCB8Y2IEVZYAAQWRKIDEGUG9PBNQPIJ4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XDTVKZBZPC9ICG1UOMLUY29TAW
5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZFDTLFBI8L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWBW46DGFZAZ4KICAGIDXCIG1
UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18XDTVKZXBZIIIBUYW1LPSJZXXMIHNVDXJJZVJLZJ0IR2F0ZXDHEV8WDDLMY2DTIIB0YXJNZXRSZ
WY9IKFJDGL2AXR5XZB1MXWCTYIIC8+CIAGICA8YNTBTPJLBMRFDMVUDCBPZD0IRXZLBNRFRMDB1CDI

VDXRNB2LUZZ5GBG93XZFMMHJ1M2M8L2JWBW46B3V0Z29PBM+CIAGICA8L2JWBW46DGFZAZ4KICAGIDXCIG1UONNL CXVLBMNLRMXVDYBPZ
D0IRMXVD18WYMP3BZZ2IIBZB3VYY2VSWY9IKDHG6V3YXLFMD0CDRMCISIDGDFYZ2V0UMVMP5JBY3RPDML0EV8WDQWXXDUII A VPGOGICA
GPGJWBW46DGFZAYBPZD0IQWN0AXZPDHLMXG3YTHLZSIGBMFTZT0IQ29SBGVJDCBUAW1LLCBHY2NVDW50IHJLCXVLC3RPMCMIZEW00HVC
3QGC2VUZGLUZYWGHDHJHZM2PYBY0BYBEQYJMTA7KE11BHRPCGXLIEVZ3MP1J4KICAGICAGPGJWBW46AW5JB21PBM+CIAGICA8L2JWBW46D
4PC9ICG1UOMLUY29TAW5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZF5N5W50YJG8L2JWBW46B3V0Z29PBM+CIAGICA8L2JWBW46D
GFZAZ4KICAGIDXCIG1UONNL CXVLBMNLRMXVDYBPZD0IRMXVD18XBG51DJB4IIBZB3VYY2VSWY9IKV2Z5W0XZBSYXZJOTEIHRHMDLDFJ
LZJ0IQWN0AXZPDHLMXG3YTHLZSIGLZ4KICAGIDXCIG1UONNL CXVLBMNLRMXVDYBPZD0IRMXVD18XETVUAGI4IIBZB3VYY2VSWY9IKFJD
GL2AXR5XZF4N2E4ZWIHRHMDLDFJLZJ0IR2F0ZXDHEV8WDZLPCGX2IIAVPGOGICAGPGJWBW46ZXXHJBHVZAXZLR2F0ZXDHE8BPZD0IR2F
0ZXDHEV8WDZLPCGX2IIBUYW1LPSJYXMGCMVXDWDZDCBMC9TIGFIBM9YBWF5IHRBPBUVCGXHY2U/IJ4KICAGICAGPGJWBW46AW5JB21PB
MC+RMXVD18XETVUAGI4PC9ICG1UOMLUY29TAW5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZB4MJZ4Y2E8L2JWBW46B3V0Z29PBM
+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMDK3ZTNTYTWVYNTBTPVDXRN2LUZZ4KICAGIDWVYNTBTPLEGN5DXNPDMMVHYXRLD2F5P
GOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZB4MJZ4Y2E8L2JWBW46B3V0Z29PBM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMTJ
IHRHMDLDFJLZJ0IR2F0ZXDHEV8WD25PBXG1IIAVPGOGICAGPGJWBW46C6GFYWXSWXHYXRLD2F5IGLKPSJHYXRLD2F5XZF3BMLTEDUIP
GOGICAGICA8YNTBTPPBMNVBLUZZ5GBG93XZB4MJZ4Y2E8L2JWBW46AW5JB21PBM+CIAGICAGIDXCIG1UOM91DGDVAW5NPGOGICAGICA8Y
NTBTPVDXRN2LUZZ5GBG93XZF1YMIJ1A3U8L2JWBW46B3V0Z29PBM+CIAGICA8L2JWBW46C6GFYWXSWXHYXRLD2F5P GOGICAGPGJWBW4
6Z5W5KRXZLBNQGAQW9IKV2Z5W0XZFJCMV1AMMIIG5HBWU9ILN0B3AIPGOGICAGICA8YNTBTPPBMNVBLUZZ5GBG93XZA5N2UZBWE8L2JWB
W46AW5JB21PBM+CIAGICA8L2JWBW46Z5KRXZLBNQ+CIAGICA8YNTBTPPZXF1Z5W5JZUSB3CGAWQ9IKZ5B3DFMDK3ZTNTY5IGBMFTZT0
ITM8IHNVDXJZVJLZJ0IR2F0ZXDHEV8WDZLPCGX2IIB0YXJNZXRSZY9IKV2Z5W0XZFJCMV1AMMIIC8+CIAGICA8YNTBTP0YXNRIGLK
SJB3Y3RPDML0EV8X2930GYF1IBUYW1LPSJSZWNVCMQGUG0Z50AW5FIEHNC2GGY29TCHJVBWLZSAOQWRKIDEGUG9PBNQPIJ4KICAGICA
GPGJWBW46AW5JB21PBM+CIAGICA8L2JWBW46B3V0Z29PBM+CIAGICAGIDXCIG1UOM91DGDVAW5NPKZSB3DFMTJ
2JWBW46B3V0Z29PBM+CIAGICA8L2JWBW46DGFZAZ4KICAGIDXCIG1UONNL CXVLBMNLRMXVDYBPZD0IRMXVD18XMD6EM84IIBZB3VYY2V
SZWY9IKDHG6V3YXLFMDUAW14NSIGDGFYZ2V0UMVMP5JBY3RPDML0EV8X2930GYF1IAVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLK
SJGBG93XZA1Z3HUC2WIIHNVDXJZVJLZJ0IR2F0ZXDHEV8WD25PBXG1IIB0YXJNZXRSZY9IKFJDGL2AXR5XZF0ZJNND2MIIC8+CIAGICA
8YNTBTPZXXJ2AWNLVGFZAYBPZD0IQWN0AXZPDHLMXG3YTHLZSIGBMFTZT0IQ29SBGVJDCBUAW1LLCBHY2NVDW50IHJLCXVLC3RPMCMIZEW00HVC
XN0IJ4KICAGICAGPGJWBW46AW5JB21PBM+CIAGICA8L2JWBW46B3V0Z29PBM+CIAGICA8YNTBTPVDXRN2LUZZ5GBG93XZB4MJZ4Y2E8L2JWBW46C6GFYWXSWXHYXRLD2F5IGLKPSJHYXRLD2F5XZF3BMLTEDUIP
3XZFN2DZ48DU8L2JWBW46B3V0Z29PBM+CIAGICA8L2JWBW46C2VYDMLJZVRHC2S+CIAGICA8YNTBTP0YXNRIGLKPSJBY3RPDML0EV8WD
DVOAJLMIIBUYW1LPSJRDWVYESBH2ZFPBNN0IFBYAXZFC2MGQWXLNCRZIJ4KICAGICAGPGJWBW46AW5JB21PBM+CIAGICA8L2JWBW46C6GFZ
ICG1UOMLUY29TAW5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZFJMMFVYNE8L2JWBW46B3V0Z29PBM+CIAGICA8L2JWBW46DGFZAZ
4KICAGIDXCIG1UONNL CXVLBMNLRMXVDYBPZD0IRMXVD18XZ3C1EGW1IIBZB3VYY2VSWY9IKFJDGL2AXR5XZF0ZJNND2MIHRHMDLDFJ
LZJ0IQWN0AXZPDHLMHQ1AG05ZIIIGLZ4KICAGIDXCIG1UOMV4Y2X1C2L2ZUDHDG6V3YXKGAWQ9IKDHG6V3YXLFMDDIAGVYYYIGBMFTZT0IR
GLKIHROZSBOB3N0IHDPDGGUHHJPDIBFC2NHBGF0AW9UJHJ1BIEQ3N5BMM/IJ4KICAGICAGPGJWBW46AW5JB21PBM+CIAGICA8L2JWBW46C6GFZ
XPC9ICG1UOMLUY29TAW5NPGOGICAGICA8YNTBTPPBMNVBLUZZ5GBG93XZFMMHJ1M2M8L2JWBW46AW5JB21PBM+CIAGICAGIDXCIG1UO
M91DGDVAW5NPKZSB3DFMDG9RY2M0EJWVYNTBTPVDXRN2LUZZ4KICAGIDWYNTBTPLEGN5DXNPDMMVHYXRLD2F5P GOGICAGPGJWBW46C2V
XDWVUY2VGBG93IGLKPSJGBG93XZFJMMFVYNEIHNVDXJZVJLZJ0IQWN0AXZPDHLMHQ1AG05ZIIIGDGFYZ2V0UMVMP5JHYXRLD2F5XZA3Y
MHLMMIIC8+CIAGICA8YNTBTPPZXF1Z5W5JZUSB3CGAWQ9IKZ5B3DFMWMYVCNUZYYIGC291CMNLUMVMP5JBY3RPDML0EV8WDQWXXDUII B
0YXJNZXRSZY9IKDHG6V3YXLFMDDIAGVYYYIGLZ4KICAGIDXCIG1UONRHC2SGAWQ9IKFJDGL2AXR5XZF0ZJTOHKIIG5HBWU9ILJLY29YZ
CBQCM2RXNJIEFJY291BNQGYWNJZXNZAW5NIEHHC2HLCYAOWYRKIDEGCG9PBNQPIJ4KICAGICAGPGJWBW46AW5JB21PBM+CIAGICA8L2JWBW46C6GFZ
JY2R6PC9ICG1UOMLUY29TAW5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZF3EDYICGU8L2JWBW46B3V0Z29PBM+CIAGICA8L2JWB
W46DGFZAZ4KICAGIDXCIG1UONNL CXVLBMNLRMXVDYBPZD0IRMXVD18W2TJY2R6IIBZB3VYY2VSWY9IKDHG6V3YXLFMDDIAGVYYYIGDGF
YZ2V0UMVMP5JBY3RPDML0EV8XCNDYBTH5IIAVPGOGICAGPGJWBW46DGFZAYBPZD0IQWN0AXZPDHLMFGP6Z213AIIIGBMFTZT0IQ29SBGVJDC
CBJBNRLCM5HBCBHBMQGRXH0XZJUYYWGS69ZDCBJBMZVJ4KICAGICAGPGJWBW46AW5JB21PBM+CIAGICA8L2JWBW46DGFZAZ4KICAGIDXCIG1UONNL CXVLBMNLRMXVDYBPZD0IRMXVD18XW0H0AWQ3PC9ICG1UOMLUY29
TAW5NPGOGICAGICA8YNTBTPVDXRN2LUZZ5GBG93XZBNCZDWCML8L2JWBW46DGFZAZ4KICAGIDXCIG1UONNL CXVLBMNLRMXVDYBPZD0IRMXVD18XW0H0AWQ3IIBZB3VYY2VSWY9IKV2Z5W0XZAZ0ZWH6YW8IHRHMDLDFJLZJ0IQWN0AXZPDHLMFGP6Z213AIIIGLZ4KICAGIDXCIG1UONNL CXVLBMNLRMXVDYBPZD0IRMXVD18W23M3CHJIIIBZB3VYY2VSWY9IKFJDGL2AXR5XZBQEMD
20IHRHMDLDFJLZJ0IR2F0ZXDHEV8XC2X6M3LJIIAVPGOGICAGPGJWBW46DGFZAYBPZD0IQWN0AXZPDHLMXG3YTHLZSIGBMFTZT0IUMV
JB3JIKFIBVDGLHBCBZWFJB25PBMCGKEFKZCAXIHBVAW50KSI+CIAGICAGIDXCIG1UOMLUY29TAW5NPKZSB3DFMHR2MDG0AJWVYNTBTP
JPPBMNVBLUZZ4KICAGICAGPGJWBW46B3V0Z29PBM+CIAGICA8L2JWBW46DGFZAZ4KICAGIDXCIG1UOM91DGDVAW5NPGOGICAGICA8YNTBTP
WDXRN2LUZZ5GBG93XZBWN2Y3DDM8L2JWBW46B3V0Z29PBM+CIAGICA8L2JWBW46C6GFYWXSWXHYXRLD2F5P GOGICAGPGJWBW46C2VXD
WVUY2VGBG93IGLKPSJGBG93XZB0DJA4NGOIHNVDXJZVJLZJ0IR2F0ZXDHEV8XC2X6M3LJIIIB0YXJNZXRSZY9IKFJDGL2AXR5XZF5YANH
YNGUIIC8+CIAGICA8YNTBTP0YXNRIGLKPSJBY3RPDML0EV8WANZHNGJVIIBUYW1LPSJRDWVYESBH2ZFPBNN0IG90AGVYIGFSZXJ0CYI+C
IAGICAGIDXCIG1UOMLUY29TAW5NPKZSB3DFMHA3ZJ0DMZVYNTBTPPBMNVBLUZZ4KICAGICAGPGJWBW46B3V0Z29PBM+CIAGICA8L2JWBW46C6GFZ
VZXPUPC9ICG1UOM91DGDVAW5NPGOGICAGPC9ICG1UONRHC2S+CIAGICA8YNTBTPPZXF1Z5W5JZUSB3CGAWQ9IKZ5B3DFMHA3ZJ0DMYIGC
291CMNLUMVMP5JHYXRLD2F5XZFZBHOYOWMIIHRHMDLDFJLZJ0IQWN0AXZPDHLMFGP6Z2YTRIBYIGLZ4KICAGIDXCIG1UOMV4Y2X1C2L2ZUD
HDG6V3YXKGAWQ9IKDHG6V3YXLFMDWSA2RUYIIGBMFTZT0ISGFZIEYLDG6VBMFSIGHVC3QGYMVLBIHBC3NVL2YHDG6V3YXLFMDG6G6B3ROZXIGY
WXLNCRZIHJLY2VUDGX5PYI+CIAGICAGIDXCIG1UOMLUY29TAW5NPKZSB3DFM9X8B2V6BJWVYNTBTPPBMNVBLUZZ4KICAGICAGPGJWBW4
6B3V0Z29PBM+CIAGICA8L2JWBW46B3V0Z29PBM+CIAGICA8YNTBTPVDXRN2LUZZ5GBG93XZF1YMI3A2Q8L2JWBW46B
3V0Z29PBM+CIAGICA8L2JWBW46ZXXHJBHVZAXZLR2F0ZXDHE4T4KICAGIDXCIG1UONNL CXVLBMNLRMXVDYBPZD0IRMXVD18X3FVZXPUIIB
ZB3VY2VSWY9IKFJDGL2AXR5XZBQDME0YM8IHRHMDLDFJLZJ0IR2F0ZXDHEV8XZ2XRZG5IIIAVPGOGICAGPGJWBW46AW5JB21PBM+CIAGICA8L2JWBW46C6GFZAYBPZD0IQ
WN0AXZPDHLMFGXRODZ5ZIIIGBMFTZT0IUMVJB3KIEJLYWVNBMLUZYB8C3NVL2YHDG6V3YXLFMDG6G6B3ROZXIGYV0YXZPB3JZTCHHZGQMS
WB2LUDCKIPGOGICAGICA8YNTBTPPBMNVBLUZZ5GBG93XZF2B2TRNH08L2JWBW46AW5JB21PBM+CIAGICAGIDXCIG1UOM91DGDVAW5N
KZSB3DFMTQXNGW20TAVYNTBTPVDXRN2LUZZ4KICAGIDWYNTBTP0YXNRPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZF
2B2TRNH0IIG5HBWU9IILLCYIGC291CMNLUMVMP5JHYXRLD2F5XZFN8GKBMIIIHRHMDLDFJLZJ0IQWN0AXZPDHLMFGXRODZ5ZIIIGLZ4K
ICAGIDXCIG1UOMVUZE2V5W5IGLKPSJFDMVUDF8WCGNRAJRIIIBUYW1LPSJTDG9WIJ4KICAGICAGPGJWBW46AW5JB21PBM+CIAGICA8L2JWBW46C6GFZAYBPZD0IQ
IN2TKPC9ICG1UOMLUY29TAW5NPGOGICAGPC9ICG1UOMVUZE2V5W5P GOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZF1YMI3A
2QIIG5HBWU9IK5VIBZB3VYY2VSWY9IKDHG6V3YXLFMDWSA2RUYIIGDGFYZ2V0UMVMP5JFDMVUDF8WCGNRAJRII A VPGOGICAGPGJWBW4

[illegible]

XNHB1ANNVIAVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZE3NHU3CZIIHNVDXJJZVJLZJ0IQWN0AXZPDHLMFTDODQ30
CIGDGFYZ2V0UMVMP5JBY3RPDML0EV8XM3NWDUMUZIIVPGOGICAGPGJWBW46C2VVDMLJZVRHC2SGAWQ9IKFJDGL2AXR5XZEZ3B2ZTMIIG5
HBWU9IKDLBMVYXRLEIENVCNJLBGF0ZWQGMVOYXPB3IGTM90AWPY2F0AW9UIJ4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XNZR1N
3MYPYC9ICG1UOMLUY29TAW5NPGOGICAGICA8YNTBTPPBMNVBWL0UZZ5GBG93XZFHEMLZOWI8L2JWBW46AW5JB21PBMCM+CIAGICAGIDIXICG1
UOMLUY29TAW5NPKZSB3DFMWC0Y3G4EJWVYNTBTPPBMNVBWL0UZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18WZNH2NTVRPC9ICG1UO
M91DGDVAW5NPGOGICAGPG9ICG1UONNLCNZPY2VUYXNRP0GICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZFHEMLZOWIIHNVDXJ
JZVJLZJ0IQWN0AXZPDHLMFTAWBTF1ZIIIGDGFYZ2V0UMVMP5JBY3RPDML0EV8XM3NWDUMUZIIVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93I
GLKPSJGBG93XZFNNNGN4OHOIHHNVDXJJZVJLZJ0IQWN0AXZPDHLMFTRDWDPZBYIGDGFYZ2V0UMVMP5JBY3RPDML0EV8XM3NWDUMUZIIVPGO
GICAGPGJWBW46Z5W5KXZLBNQGAWQ9IKV2Z5W50XZBIOXNUCJUIIG5HBU9IILN0B3AIPGOGICAGICA8YNTBTPPBMNVBWL0UZZ5GBG93XZAZ30
HY1NWS8L2JWBW46AW5JB21PBMCM+CIAGICA8L2JWBW46Z5W5KXZLBNQ+CIAGICA8YNTBTPPZXXF1Z5W5JZUSB3CGAWQ9IKZSB3DFMDC4DJU
1AYIGC291CMNLUMVMP5JBY3RPDML0EV8XM3NWDUMUZIIB0YXJNZXRSZY9IKV2Z5W50XZBIOXNUCJUIIC8+CIAGICA8YNTBTPPZDGFYDEVZ2
W50IGLKPSJFDMVUDF8WDH6NJWIIBUYW1LPSJMYXRLCMFSTW92Z2W1LBNQGQWXLNQP0GOGICAGICA8YNTBTPPVDXRN82LUZZ5GBG93XZB
YC2F1A3Q8L2JWBW46B3V0Z29PBMCM+CIAGICAGIDIXICG1UONNP225HBEV2Z5W50RGVMAW5PDGLVBIBPZD0IU2LBNBMFSRXZLBNREZWPBML0A
W9UXZFVMNJZJMSIIC8+CIAGICA8L2JWBW46C3RHCNRFDMVUD4KICAGIDIXICG1UONRHC2SGAWQ9IKFJDGL2AXR5XZFXEXF6D2YIIG5HBU
9IKNVBGXLY3QDGLTZW5G291CMNL0CBHBMQGVZDGLUYXRPB24GZM9YIG1VDMVTZ5W50I4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD
18WCNNH0DTPC9ICG1UOMLUY29TAW5NPGOGICAGICA8YNTBTPVDXRN82LUZZ5GBG93XZAYZ3MWDW88L2JWBW46B3V0Z29PBMCM+CIAGICA
8L2JWBW46DGFZAZ4KICAGIDIXICG1UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18WCNNH0DTP0IBZB3VY2V5Z5WY9IKV2Z5W50XZB0D302MJAII
HRH0CMLDFJLZJ0IQWN0AXZPDHLMF5XCP3ZIIIGLZ4KICAGIDIXICG1UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18WMMDMZHHVVIIBZB3VY2V
SZWY9IKFJDGL2AXR5XZFXEXF6D2YIHRH0CMLDFJLZJ0IR2F0ZXDHEV8XDHE1BZYWIIAVPGOGICAGPGJWBW46CGFYWWSZXWYXRDL2F5I
GLKPSJHYXRDL2F5XZF0CTVNVJAIPOGICAGICA8YNTBTPPBMNVBWL0UZZ5GBG93XZAYZ3MWDW88L2JWBW46AW5JB21PBMCM+CIAGICAGIDIX
ICG1UOM91DGDVAW5NPKZSB3DFMHNJ6NM900TWVYNTBTPPVDXRN82LUZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18XMGPCZCG5WPC9IC
G1UOM91DGDVAW5NPGOGICAGPG9ICG1UONBHCMSBGVSR2F0ZXDHE4KICAGIDIXICG1UONRHC2SGAWQ9IKFJDGL2AXR5XZB0NMHIEAIIIG5
HBWU9ILF12XJ5TEFNYWLU3CQGREMU3LUYYBBBGVYDHMIPGOGICAGICA8YNTBTPPBMNVBWL0UZZ5GBG93XZBYEJZVDDK8L2JWBW46AW5JB
21PBMCM+CIAGICAGIDIXICG1UOM91DGDVAW5NPKZSB3DFMWSMHQ0ATWVYNTBTPPVDXRN82LUZZ4KICAGIDWVYNTBTPP0YXNRP0GICAGPGJ
WBW46C2VXDWVUY2VGBG93IGLKPSJGBG93XZBYEJZVDDKIHHNVDXJJZVJLZJ0IR2F0ZXDHEV8XDHE1BZYWIIAB0YXJNZXRSZY9IKFJDGL2A
XR5XZB0NMHIEAIIIC8+CIAGICA8YNTBTPPLEGSDXNPMVMHYXRDL2F5IGLKPSJHYXRDL2F5XZE4DWLKEIXMIG5HBU9IKLZIHROZSBZ3V
YY2UGB2YGTGF0XJHBCBNB3ZLBWVUDCB0AGUGSG9ZDCB2B5KDNW0AW5NIERDIFN5BMM/IJ4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD
18XZGWWDDRP9ICG1UOMLUY29TAW5NPGOGICAGICA8YNTBTPPBMNVBWL0UZZ5GBG93XZFTNTDRNJ8L2JWBW46AW5JB21PBMCM+CIAGICA
GIDIXICG1UOM91DGDVAW5NPKZSB3DFMHNJBDZRDWVYNTBTPPVDXRN82LUZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18WEXQ0B3P
C9ICG1UOM91DGDVAW5NPGOGICAGPG9ICG1UOMV4Y2X1C2L2ZUDHDGV3YXK+CIAGICA8YNTBTPPZXXF1Z5W5JZUSB3CGAWQ9IKZSB3DFMWR
SMHQ0ASIGC291CMNLUMVMP5JBY3RPDML0EV8WDDZ0YNPWIIB0YXJNZXRSZY9IKDHDGV3YXLFMTH1AWR5CYIGLZ4KICAGIDIXICG1UONRHC
2SGAWQ9IKFJDGL2AXR5XZFXCNWKNW4IIG5HBU9ILF12XJ5TEFNYWLU3CQGRXHMMAWQWXLNCRZIJ4KICAGICAGPGJWBW46AW5JB21PBMCM
+RMXVD18XMGPCZCG5WPC9ICG1UOMLUY29TAW5NPGOGICAGICA8YNTBTPPVDXRN82LUZZ5GBG93XZB2AMHYB2K8L2JWBW46B3V0Z29PBMCM+C
IAGICA8L2JWBW46DGFZAZ4KICAGIDIXICG1UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18XMGPCZCG5WIIIBZB3VY2V5Z5WY9IKDHDGV3YXLFMXR
XNW82MCIGDGFYZ2V0UMVMP5JBY3RPDML0EV8XCXFJZDVUIIIVPGOGICAGPGJWBW46DGFZAYBPZD0IQWN0AXZPDHLMFJ2M2FUCSIGBMFTZ
T0TUXVLCNKQGWDHAW5ZDCBMYXRLCMFSIE1VDMVTZ5W50EF5XZJ0CYI+CIAGICAGIDIXICG1UOMLUY29TAW5NPKZSB3DFMXVIYVNRD0TWVYNT
BTPPBMNVBWL0UZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18XBTU3AZYWPC9ICG1UOM91DGDVAW5NPGOGICAGPG9ICG1UONRHC2S+C
IAGICA8YNTBTPPZXXF1Z5W5JZUSB3CGAWQ9IKZSB3DFMXVIYVNRDSIGC291CMNLUMVMP5JHYXRDL2F5XZF3BMLTEDUIIHRH0CMLDFJLZJ0
IQWN0AXZPDHLMFJ2M2FUCSIGLZ4KICAGIDIXICG1UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18XBTU3AZYWIIBZB3VY2V5Z5WY9IKFJDGL2A
XR5XZBYDJNHBNEIHRH0CMLDFJLZJ0IR2F0ZXDHEV8XOHPVZHLZIIIVPGOGICAGPGJWBW46DGFZAYBPZD0IQWN0AXZPDHLMFDFHATZRZCI
GBMFTZT0IUMVJB3JKEI0DFN5BMMGBGVKIHRIEXHDGVYVWGTW92Z2W1LBNQGFKEFKZCAXIFBVAW50KSI+CIAGICAGIDIXICG1UOMLUY29TA
W5NPKZSB3DFMHNJBDZRDWVYNTBTPPBMNVBWL0UZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18WCTZOM205PC9ICG1UOM91DGDVAW5
NPGOGICAGPG9ICG1UONRHC2S+CIAGICA8YNTBTPPZXXF1Z5W5JZUSB3CGAWQ9IKZSB3DFMHNJBDZRD0IGBMFTZT0TWMVY9IKDHDGV3YXLFV
WY9IKDHDGV3YXLFMTH1AWR5CYIGDGFYZ2V0UMVMP5JBY3RPDML0EV8WMMFPMNTKIIIVPGOGICAGPGJWBW46C2VXDWVUY2VGBG93IGLKPSJ
GBG93XZBXNMGZAJKIIHNVDXJJZVJLZJ0IQWN0AXZPDHLMFDFHATZRZCIGDGFYZ2V0UMVMP5JBY3RPDML0EV8XAW10AHMSIIIVPGOGICAGP
GJWBW46Z5W5KXZLBNQGAWQ9IKV2Z5W50XEYNWD3AMIIG5HBU9IILN0B3AIPGOGICAGICA8YNTBTPPBMNVBWL0UZZ5GBG93XZB5DDRVD0C
8L2JWBW46AW5JB21PBMCM+CIAGICA8L2JWBW46Z5W5KXZLBNQ+CIAGICA8YNTBTPPZXXF1Z5W5JZUSB3CGAWQ9IKZSB3DFMHL0N84NYIGB
MFTZT0TMIHHNVDXJJZVJLZJ0IR2F0ZXDHEV8XOHPVZHLZIIIVPGOGICAGPGJWBW46DGFZAYBPZD0IQWN0AXZPDHLMFDFHATZRZCI
SDXNPMVMHYXRDL2F5IGLKPSJHYXRDL2F5XZBNETU0DHKIIIG5HBU9IKLZIERLC3RPMBF0AW9UIHDOZXJLIEV4ZMLSIG9JY3VY2Z8IPGOGI
CAGICA8YNTBTPPBMNVBWL0UZZ5GBG93XZB2AMHYB2K8L2JWBW46AW5JB21PBMCM+CIAGICAGIDIXICG1UOMLUY29TAW5NPKZSB3DFMGVTMMV
ZBDWVYNTBTPPBMNVBWL0UZZ4KICAGICAGPGJWBW46B3V0Z29PBMCM+RMXVD18XY2Z4MNA4PC9ICG1UOM91DGDVAW5NPGOGICAGICA8YNTBTP
JPVDXRN82LUZZ5GBG93XZBIAZHQWY8L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWBW46Z5W5KXZLBNQ+CIAGICA8YNTBTPPZXXF1Z5W5JZUSB3CGAWQ9IKZSB3DFMHL0N84NYIGB
LCXVBLMNLRMXVDYBPZD0IRMXVD18WDMPOCM9PIIBZB3VY2V5Z5WY9IKFJDGL2AXR5XZFXCNWKNW4IHRH0CMLDFJLZJ0IR2F0ZXDHEV8WZ
3K1NHR5IIIVPGOGICAGPGJWBW46DGFZAYBPZD0IQWN0AXZPDHLMFGNSNJQ4ZSIGBMFTZT0IUMVJB3JKEIEXHDCBNB3ZLIEZLZCB0YBFEGZ
PBCAQWKRKIDEGUG9PBNQPIJ4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XY2Z4MNA4PC9ICG1UOMLUY29TAW5NPGOGICAGICA8YNTBTP
JPVDXRN82LUZZ5GBG93XZFUW5PDZM8L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWBW46DGFZAZ4KICAGIDIXICG1UONNLCXVBLMNLRMXVDYB
PZD0IRMXVD18XY2Z4MNA4IIBUYW1LPSJZXXMIHNVDXJJZVJLZJ0IR2F0ZXDHEV8WZ3K1NHR5IIIB0YXJNZXRSZY9IKFJDGL2AXR5XZB3B
DY0OGUIC8+CIAGICA8YNTBTPPZXXF1Z5W5JZUSB3CGAWQ9IKZSB3DFMW55BML3MYIGC291CMNLUMVMP5JBY3RPDML0EV8WY2W2NDHLIIB
0YXJNZXRSZY9IKFJDGL2AXR5XZFPBXROCKZIIIC8+CIAGICA8YNTBTPP0YXNRIIGLKPSJBY3RPDML0EV8WZ2W50IIBUYW1LPSJRDWVYE
SBBZ2FPBNN0IEXHDGVYVWGTW92Z2W1LBNQGQWXLNCRZIJ4KICAGICAGPGJWBW46AW5JB21PBMCM+RMXVD18XNTBHDZ3PC9ICG1UOMLUY29
TAW5NPGOGICAGICA8YNTBTPPVDXRN82LUZZ5GBG93XZBLBTLF3L2W8L2JWBW46B3V0Z29PBMCM+CIAGICA8L2JWBW46DGFZAZ4KICAGIDIXIC
G1UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18WZ0XZNSIIBZB3VY2V5Z5WY9IKFJDGL2AXR5XZBLYWZRBQIIRH0CMLDFJLZJ0IR2F0ZXD
HEV8WZ3K1NHR5IIIVPGOGICAGPGJWBW46Z5W5KXZLBNQGAWQ9IKV2Z5W50XZFLBG43MMGIIG5HBU9IILN0B3AIPGOGICAGICA8YNTBTPP
MNVBWL0UZZ5GBG93XZBIAZHQWY8L2JWBW46AW5JB21PBMCM+CIAGICA8L2JWBW46Z5W5KXZLBNQ+CIAGICA8YNTBTPPZXXF1Z5W5JZUSB3C
GAWQ9IKZSB3DFMGJROG05ZIIIGBMFTZT0ITM8IIHNVDXJJZVJLZJ0IR2F0ZXDHEV8WZ3K1NHR5IIIB0YXJNZXRSZY9IKV2Z5W50XZFLBG43M
MGIIC8+CIAGICA8YNTBTPPZXXF1Z5W5JZUSB3CGAWQ9IKZSB3DFMXHNMZNYIGC291CMNLUMVMP5JHYXRDL2F5XZF2KZNMZY2EIIHRH0CML
LDFJLZJ0IQWN0AXZPDHLMFJXUCDHOOCIGLZ4KICAGIDIXICG1UONNLCXVBLMNLRMXVDYBPZD0IRMXVD18XNTBHDZ3IIBZB3VY2V5Z5WY9I
KDHDGV3YXLFMWRMY3NJMSIGDGFYZ2V0UMVMP5JBY3RPDML0EV8WZ2W50IIVPGOGICAGPGJWBW46DGV4DEFUBM90YXRPB24GAWQ9ILR

LEHRB8M5VDGF0AW9UXZBPNDN3MZKIPGOGICAGICA8YNB8TBJP0ZXH0PKNOZWNRIGLUDGVYBMFSIGHVC3QGYWDHAW5ZDCBTCGVHCNBOAXNOL
CBNYWYBYWYGUMVYNA0CNKGTW9KLCBQCM2RXN1LCBEQ1N5BMM5IGFUCZBMXYRLCMFSIE1VDMVPTZW50PC9ICG1UONRLEHQ+CIAGICA812J
WBW46DGV4DEFUBM90YXRPB24+CIAGICA8YNB8TBJPHC3NVY2LHDGLVBI8PZD0IQXNZB2NPYXRPB25FMTVYCHNRMCIGC291CMNLMVMVPSJBY
3RPDML0EV8WANZHNG3V1IB0YXJNZXRSZY9ILRLHRB8M5VDGF0AW9UXZBPNDN3MZKIIC8+CIAGPC9ICG1UONBYB2NLC3M+CIAGPGJWBW5
KATPCUE10RGLHZ3JHBSBPZD0QLBNTKRPYWDYWFMSI+CIAGICA8YNB8TBMRP0KJQTU5QBGFUZSBPZD0QLBNTLBSYW5LXZE1IGJWBW5FB
GVTZW50PSJQCM9JZXNZXF8BMVNDG0IPGOGICAGICA8YNB8TBMRP0KJQTU5FZGDLIGLKPSJGBG93XZE1MGF3MNDZFZGKIIGJWBW5FBGVTZW5
0PSJGBG93XZE1MGF3MNCIPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI1NTAI1HK9IJIWNUZUIIC8+CIAGICAGICAGPGRPONDEHBVW50I
HG9IJJU1MCIGET0IMJAYMCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZGK6QLBNTKVKZ2UGAWQ9IKZSB3DFMXH
XMZN2N19KASIGYNB8TBKVSZW1LBNQ9IKZSB3DFMXHXMZN2NYI+CIAGICAGICAGPGRPONDEHBVW50IHG9IJJU3NSIGET0IMJEWMCIGLZ4KI
CAGICAGICA8ZGK6D2F5CG9PBNQGED0INZKWIIB5PSIYMTAWIIAVPGOGICAGICA8L2JWBW5KATPCUE10RWRNZT4KICAGICAGPGJWBW5KATP
CUE10RWRNZSBPZD0IRMVXD18WYMS4AJLMX2RPIIBICG1URWLWBUVDD0IRMVXD18WYMS4AJLMJ4KICAGICAGICA8ZGK6D2F5CG9PBNQGE
D0INTCWIIB5PSIXODM1IIAVPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI1NZAI1HK9IJE40DAIIC8+CIAGICAGICAGPGRPONDEHBVW50I
0IHG9IJJU1MIGET0IMTG4MCIGLZ4KICAGICAGICA8YNB8TBMRP0KJQTU5MYWJLBD4KICAGICAGICAGIDKXYPZC3VUZHMGED0INTC4IIB5P
SIXODUZIIB3AWR0AD0IMTUIIGHLAWDODD0IMTQIIC8+CIAGICAGICAGPC9ICG1UZGK6QLBNTKXHYMVSPGOGICAGICA8L2JWBW5KATPCUE1
0RWRNZT4KICAGICAGPGJWBW5KATPCUE10RWRNZSBPZD0IRMVXD18WZWXZNSX2RPIIBICG1URWLWBUVDD0IRMVXD18WZWXZNSI4KI
CAGICAGICA8ZGK6D2F5CG9PBNQGED0INTUWIIIB5PSIXOTQWIIAVPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI1NTAI1HK9IJE4MTUIIC8
+CIAGICAGIDWVYNB8TBMRP0KJQTU5FZGDLPGOGICAGICA8YNB8TBMRP0KJQTU5FZGDLIGLKPSJGBG93XZFUEW5PDZNFZGKIIGJWBW5FBGVTZ
W50PSJGBG93XZFUEW5PDZMIPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI3NTAI1HK9IJE4MTAIIC8+CIAGICAGICAGPGRPONDEHBVW50I
0IHG9IJJYOTAI1HK9IJE4MTAIIC8+CIAGICAGICAGPGRPONDEHBVW50IHG9IJJYOTAI1HK9IJE4MTAIIC8+CIAGICAGIDWVYNB8TBMRP0
KJQTU5FZGDLPGOGICAGICA8YNB8TBMRP0KJQTU5FZGDLIGLKPSJGBG93XZFJZNGVCDHFZGKIIGJWBW5FBGVTZW50PSJGBG93XZFJZNGVCDG
IPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI10TUI1HK9IJE4MTAIIC8+CIAGICAGICAGPGRPONDEHBVW50IHG9IJJY1MCIGET0IMTGXM
CIGLZ4KICAGICAGICA8YNB8TBMRP0KJQTU5MYWJLBD4KICAGICAGICAGIDKXYPZC3VUZHMGED0INJEXIIB5PSIXNZKZIIIB3AWR0AD0IMTG
IIGHLAWDODD0IMTQIIC8+CIAGICAGICAGPC9ICG1UZGK6QLBNTKXHYMVSPGOGICAGICA8L2JWBW5KATPCUE10RWRNZT4KICAGICAGPGJWB
W5KATPCUE10RWRNZSBPZD0IRMVXD18WMDPOMC9PX2RPIIBICG1URWLWBUVDD0IRMVXD18WMDPOMC9PIJ4KICAGICAGICA8ZGK6D2F5CG9
PBNQGED0INDKWIIB5PSIXODEWIIAVPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI1NDUI1HK9IJE4MTAIIC8+CIAGICAGIDWVYNB8TBMRP0
KJQTU5FZGDLPGOGICAGICA8YNB8TBMRP0KJQTU5FZGDLIGLKPSJGBG93XZB5DDRVD0DFZGKIIGJWBW5FBGVTZW50PSJGBG93XZB5DDRVD0C
IPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI3MDAI1HK9IJE2NZUIIC8+CIAGICAGICAGPGRPONDEHBVW50IHG9IJJCMCIGET0IMT0M
CIGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0I0DYIIB5PSIXNZQWIIAVPGOGICAGICAGIDXCIG1UZGK6QLBNTKXHYMVSPGOGICAGICA
GICAGPGRJOKJVDW5KCYB3I3MDGI1HK9IJE3MDQI1HDPZHR0PSIXNSIGAGVPZ2H0PSIXNCIGLZ4KICAGICAGICA8L2JWBW5KATPCUE10T
GF1ZW+CIAGICAGIDWVYNB8TBMRP0KJQTU5FZGDLPGOGICAGICA8YNB8TBMRP0KJQTU5FZGDLIGLKPSJGBG93XZBXNMGZJLFGZKIIGJWBW5
FBGVTZW50PSJGBG93XZBXNMGZAJKIPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI5NJAI1HK9IJE2NTAIIC8+CIAGICAGICAGPGRPONDE
HBVW50IHG9IJJYNZAI1HK9IJE2NTAIIC8+CIAGICAGICAGPGRPONDEHBVW50IHG9IJJYNZAI1HK9IJE2NTAIIC8+CIAGICAGIDWVYNB
TBMRP0KJQTU5FZGDLPGOGICAGICA8YNB8TBMRP0KJQTU5FZGDLIGLKPSJGBG93XZBZY2W2A3RFZGKIIGJWBW5FBGVTZW50PSJGBG93XZBZY
2W2A3QIPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI3MJUI1HK9IJE2NTAIIC8+CIAGICAGICAGPGRPONDEHBVW50IHG9IJJ2MCIGET0
IMTY1MCIGLZ4KICAGICAGICA8YNB8TBMRP0KJQTU5MYWJLBD4KICAGICAGICAGIDKXYPZC3VUZHMGED0INZG0IIB5PSIXNJMYIIB3AWR0A
D0IMTGIIGHLAWDODD0IMTQIIC8+CIAGICAGICAGPC9ICG1UZGK6QLBNTKXHYMVSPGOGICAGICA8L2JWBW5KATPCUE10RWRNZT4KICAGICA
GPGJWBW5KATPCUE10RWRNZSBPZD0IRMVXD18XBTU3AZYWX2RPIIBICG1URWLWBUVDD0IRMVXD18XBTU3AZYWIJ4KICAGICAGICA8ZGK6D
2F5CG9PBNQGED0INJYWIIB5PSIXNTAWIIAVPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI3MDAI1HK9IJE1MDAIIC8+CIAGICAGICAGPGR
PONDEHBVW50IHG9IJJCMCIGET0IMTYINSIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZGK6QLBNTKVKZ2UGA
WQ9IKZSB3DFMXVIYNVRDV9KASIGYNB8TBKVSZW1LBNQ9IKZSB3DFMXVIYNVRDSI+CIAGICAGICAGPGRPONDEHBVW50IHG9IJJYXMCIGET0
IMTMXNSIGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0INJEWIIB5PSIXNDYWIIVAVPGOGICAGICA8L2JWBW5KATPCUE10RWRNZT4KICAGI
CAGPGJWBW5KATPCUE10RWRNZSBPZD0IRMVXD18XMGPCZG5WX2RPIIBICG1URWLWBUVDD0IRMVXD18XMGPCZG5WIJ4KICAGICAGICA8ZGK
6D2F5CG9PBNQGED0INDQWIIB5PSIXNJCI1IAVPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI0NDAI1HK9IJE3NZAIIC8+CIAGICAGIDWVY
NB8TBMRP0KJQTU5FZGDLPGOGICAGICA8YNB8TBMRP0KJQTU5FZGDLIGLKPSJGBG93XZFKBD0NGLFZGKIIGJWBW5FBGVTZW50PSJGBG93XZF
KBD0NGKIPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI2MJAI1HK9IJE2NTAIIC8+CIAGICAGICAGPGRPONDEHBVW50IHG9IJJ3NSIGE
T0IMTY1MCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZGK6QLBNTKVKZ2UGAWQ9IKZSB3DFMHJ6NM900V9KASI
GYNB8TBKVSZW1LBNQ9IKZSB3DFMHJ6NM900SI+CIAGICAGICAGPGRPONDEHBVW50IHG9IJJQ2NSIGET0IMTY1MCIGLZ4KICAGICAGICA8Z
GK6D2F5CG9PBNQGED0INTIWIIB5PSIXNJUWIIAVPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI0NDAI1HK9IJE3NZAIIC8+CIAGICAGIDWVYNB8TBMRP0KJQTU5FZGDLPGOGIC
PZD0IRMVXD18WMDZMHVX2RPIIBICG1URWLWBUVDD0IRMVXD18WMDZMHVVIJ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IMZYWIIB5P
SIXNJUWIIAVPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI0MTUI1HK9IJE2NTAIIC8+CIAGICAGIDWVYNB8TBMRP0KJQTU5FZGDLPGOGIC
GICA8YNB8TBMRP0KJQTU5FZGDLIGLKPSJGBG93XZBYC2F1A3RFZGKIIGJWBW5FBGVTZW50PSJGBG93XZBYC2F1A3QIPGOGICAGICAGIDXKA
TP3YXLWB2LUDCB4PSIYMDGI1HK9IJE2NTAIIC8+CIAGICAGICAGPGRPONDEHBVW50IHG9IJJ2MCIGET0IMTY1MCIGLZ4KICAGICAGPC9
ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZGK6QLBNTKVKZ2UGAWQ9IKZSB3DFMDC4DJU1A19KASIGYNB8TBKVSZW1LBNQ9IKZSB3DFM
DC4DJU1AYI+CIAGICAGICAGPGRPONDEHBVW50IHG9IJJMWMJAI1HK9IJEWNDAIIC8+CIAGICAGICAGPGRPONDEHBVW50IHG9IJJMXNJI
I1HK9IJEWNDAIIC8+CIAGICAGIDWVYNB8TBMRP0KJQTU5FZGDLPGOGICAGICA8YNB8TBMRP0KJQTU5FZGDLIGLKPSJGBG93XZFNNGN40HPFZ
GKIIGJWBW5FBGVTZW50PSJGBG93XZFNNGN40HOIPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSIYNZGWIIB5PSIXMTYWIIVAVPGOGICAGICA
GIDXKATP3YXLWB2LUDCB4PSIYODUWIIB5PSIXMTYWIIVAVPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSIYODUWIIB5PSIXMDCWIIAVPGOGI
CAGICAGIDXKATP3YXLWB2LUDCB4PSIYOTIWIIB5PSIXMDCWIIAVPGOGICAGICA8L2JWBW5KATPCUE10RWRNZT4KICAGICAGPGJWBW5KATP
CUE10RWRNZSBPZD0IRMVXD18YXPPCZLIX2RPIIBICG1URWLWBUVDD0IRMVXD18YXPPCZLIJ4KICAGICAGICA8ZGK6D2F5CG9PBNQGE
D0IMJC4MCIGET0I0TAWIIAVPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSIYODUWIIB5PSI5MDAIIC8+CIAGICAGICAGPGRPONDEHBVW50I
0IHG9IJJ4NTAI1HK9IJEWMTAIIC8+CIAGICAGICAGPGRPONDEHBVW50IHG9IJJ5MJAI1HK9IJEWMTAIIC8+CIAGICAGIDWVYNB8TBMRP0
KJQTU5FZGDLPGOGICAGICA8YNB8TBMRP0KJQTU5FZGDLIGLKPSJGBG93XZE3NHU3CZJFZGKIIGJWBW5FBGVTZW50PSJGBG93XZE3NHU3CZI
IPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSIYNZGWIIB5PSIXMDQWIIAVPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSIYOTIWIIB5PSIXM
DQWIIAVPGOGICAGICA8L2JWBW5KATPCUE10RWRNZT4KICAGICAGPGJWBW5KATPCUE10RWRNZSBPZD0IRMVXD18WANBUOGOYX2RPIIBICG1
URWLWBUVDD0IRMVXD18WANBUOGOYI4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IMJUYMCIGET0IMTA2NSIGLZ4KICAGICAGICA8ZGK6D
2F5CG9PBNQGED0IMJUYMCIGET0IMTE2MCIGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IMJY4MCIGET0IMTE2MCIGLZ4KICAGICAGICA
8YNB8TBMRP0KJQTU5MYWJLBD4KICAGICAGICAGIDKXYPZC3VUZHMGED0IMJU4NCIGET0IMTEZMYIGD2LKDGG9IJJU5IIBOZWLNAHQ9IJJ3I
IAVPGOGICAGICAGIDWVYNB8TBMRP0KJQTU5MYWJLBD4KICAGICAGPC9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZGK6QLBNTKVKZ2U

[illegible]

GIDWVYNBTMRPOKJQTU5MYWJLBD4KICAGICAGPC9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZGK6QLBNTKVKZ2UGAWQ9IKZSB3DFM
W9XB2V6BL9KASIGYNBTBKVSZW1LBNQ9IKZSB3DFM9XB2V6BII+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJWMCIGET0IMJUZMCIGLZ4
KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IMTE5NSIGET0IMJUZMCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZ
GK6QLBNTKVKZ2UGAWQ9IKZSB3DFMHA3ZJD0M19KASIGYNBTBKVSZW1LBNQ9IKZSB3DFMHA3ZJD0MYI+CIAGICAGICAGPGRPONDEXBVAW5
0IHG9IJUZMCIGET0IMJQ0NSIGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0INTMWIIB5PSIYNTMWIIAVPGOGICAGICAGIDKATP3YXLWB
2LUDCB4PSI2MDAIIHK9IJI1MZAIIIC8+CIAGICAGIDWVYNBTMRPOKJQTU5FZGDLPGOGICAGICA8YNTBTMRPOKJQTU5FZGDLIGLKPSJGBG9
3XZB0DJA4NGPFGZGKIIGJWBW5FBGVTZW50PSJGBG93XZB0DJA4NGOIPGOGICAGICAGIDKATP3YXLWB2LUDCB4PSIINTUIIHK9IJI10MJA
IIC8+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJK5MCIGET0IMJQYMCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1
UZGK6QLBNTKVKZ2UGAWQ9IKZSB3DFMGDZN3BYYL9KASIGYNBTBKVSZW1LBNQ9IKZSB3DFMGDZN3BYII+CIAGICAGICAGPGRPONDEXBVA
W50IHG9IJWMCIGET0IMJQYMCIGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0INTA1IIB5PSIYNDIWIIVPGOGICAGICA8L2JWBW5KATP
CUE10RWRNZT4KICAGICAGPGJWBW5KATPCUE10RWRNZSBPZD0IRMXVD18XBW0AWQ3X2RPIIBICG1URWXLBWVUDD0IRMXVD18XBW0AWQ3I
J4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IMJE4IIB5PSIYNDIWIIVPGOGICAGICAGIDKATP3YXLWB2LUDCB4PSI2MDAIIHK9IJI10MJA
IIC8+CIAGICAGIDWVYNBTMRPOKJQTU5FZGDLPGOGICAGICA8YNTBTMRPOKJQTU5FZGDLIGLKPSJGBG93XZBVA2NJNHPFZGKIIGJWBW5FB
GVTZW50PSJGBG93XZBVA2NJNHOIPGOGICAGICAGIDKATP3YXLWB2LUDCB4PSIXMJAI1IIB5PSIXMJKWIIVPGOGICAGICAGIDKATP3YXL
WB2LUDCB4PSIXNDAWIIB5PSIXMJKWIIVPGOGICAGICA8L2JWBW5KATPCUE10RWRNZT4KICAGICAGPGJWBW5KATPCUE10RWRNZSBPZD0IR
MXVD18XZJBYDTNJX2RPIIBICG1URWXLBWVUDD0IRMXVD18XZJBYDTNJIJ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IMTE4MCIGET0IMTE
4MCIGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IMTE4MCIGET0IMTI2NSIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGI
DXICG1UZGK6QLBNTKVKZ2UGAWQ9IKZSB3DFMWMYYW9ICV9KASIGYNBTBKVSZW1LBNQ9IKZSB3DFMWMYYW9ICSI+CIAGICAGICAGPGRPON
DEXBVAW50IHG9IJEWNTAIIHK9IJEYOTAIIC8+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJEWNTAIIHK9IJEYOTAIIC8+CIAGICAGIDWVY
NBTMRPOKJQTU5FZGDLPGOGICAGICA8YNTBTMRPOKJQTU5FZGDLIGLKPSJGBG93XZFNZV4BDVZGKIIGJWBW5FBGVTZW50PSJGBG93XZF
NDZV4BDUIPVGOGICAGICAGIDKATP3YXLWB2LUDCB4PSI4NTAIIHK9IJEYOTAIIC8+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJK1MCIGE
T0IMTI5MCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZGK6QLBNTKVKZ2UGAWQ9IKZSB3DFMDVNEG5ZBF9KASI
GYNBTBKVSZW1LBNQ9IKZSB3DFMDVNEG5ZBCI+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJJZNSIGET0IMTI5MCIGLZ4KICAGICAGICA8Z
GK6D2F5CG9PBNQGED0INZUWIIIB5PSIXMJKWIIVPGOGICAGICA8L2JWBW5KATPCUE10RWRNZT4KICAGICAGPGJWBW5KATPCUE10RWRNZSB
PZD0IRMXVD18XMMDEME84X2RPIIBICG1URWXLBWVUDD0IRMXVD18XMMDEME84I1J4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0INJ1IIB5P
SIXMZA1IIVPGOGICAGICAGIDKATP3YXLWB2LUDCB4PSI2MJAIIHK9IJE0MZAIIIC8+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJC1MCI
GET0IMTQZMCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZGK6QLBNTKVKZ2UGAWQ9IKZSB3DFMDK3ZTNTYV9KA
SIGYNBTBKVSZW1LBNQ9IKZSB3DFMDK3ZTNTYSI+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJJ1MCIGET0IMTMXNSIGLZ4KICAGICAGICA
8ZGK6D2F5CG9PBNQGED0INDUWIIIB5PSIXNDAWIIVPGOGICAGICAGIDKATP3YXLWB2LUDCB4PSI1MTIIHK9IJE0MDAIIIC8+CIAGICAGI
CAGPGJWBW5KATPCUE10TGFIZW+CIAGICAGICAGICA8ZG6M91BMRZIHG9IJJ10CIGET0IMTM1MSIGD2LKDG6G9IJE1IIB0ZWLNAHQ9IJE
0IIAVPGOGICAGICAGIDWVYNBTMRPOKJQTU5MYWJLBD4KICAGICAGPC9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZGK6QLBNTKVKZ
2UGAWQ9IKZSB3DFMHGYNHJYV9KASIGYNBTBKVSZW1LBNQ9IKZSB3DFMHGYNHJYSI+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJJ3NSI
GET0IMTI5MCIGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0INTG1IIB5PSIXMJKWIIVPGOGICAGICAGIDXCIG1UZGK6QLBNTKXHYMVSP
GOGICAGICAGICAGPGRJOKJVDW5KCYB4PSI1NDKIIHK9IJEYNYZIIHDPZHR0PSIXOCIGAGVPZ2H0PSIXNCIGLZ4KICAGICAGICA8L2JWBW5
KATPCUE10TGFIZW+CIAGICAGIDWVYNBTMRPOKJQTU5FZGDLPGOGICAGICA8YNTBTMRPOKJQTU5FZGDLIGLKPSJGBG93XZF5NW50YJHFZ
GKIIGJWBW5FBGVTZW50PSJGBG93XZF5NW50YJGIPGOGICAGICAGIDKATP3YXLWB2LUDCB4PSI2NJAI1HK9IJEYOTAIIC8+CIAGICAGICA
GPRPONDEXBVAW50IHG9IJJQYNSIGET0IMTI5MCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZGK6QLBNTKVKZ
2UGAWQ9IKZSB3DFMWRXNYWEF9KASIGYNBTBKVSZW1LBNQ9IKZSB3DFMWRXNYWECI+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJIWOCI
GET0IMTI5MCIGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IMJYIIB5PSIXMJKWIIVPGOGICAGICA8L2JWBW5KATPCUE10RWRNZT4KI
CAGICAGPGJWBW5KATPCUE10RWRNZSBPZD0IRMXVD18WYMP3BZZ2X2RPIIBICG1URWXLBWVUDD0IRMXVD18WYMP3BZZ2I1J4KICAGICAGICA
8ZGK6D2F5CG9PBNQGED0INDCWIIB5PSIXMDA1IIVPGOGICAGICAGIDKATP3YXLWB2LUDCB4PSI0NZAI1HK9IJEXNDAIIC8+CIAGICAGI
CAGPGRPONDEXBVAW50IHG9IJEEXMAIIHK9IJEXNDAIIC8+CIAGICAGIDWVYNBTMRPOKJQTU5FZGDLPGOGICAGICA8YNTBTMRPOKJQTU5
FZGDLIGLKPSJGBG93XZB5Y2XQDZRFZGKIIGJWBW5FBGVTZW50PSJGBG93XZB5Y2XQDZQIPGOGICAGICAGIDKATP3YXLWB2LUDCB4PSI3N
ZAI1HK9IJEWMUUIIC8+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJC3MCIGET0IMTA3MCIGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0
IODKYIIB5PSIXMDCWIIIVPGOGICAGICAGIDXCIG1UZGK6QLBNTKXHYMVSPGOGICAGICAGICAGPGRJOKJVDW5KCYB4PSI20TKIHK9IJEWM
ZGIHDPZHR0PSI2MYIAGAGVPZ2H0PSIXNCIGLZ4KICAGICAGICA8L2JWBW5KATPCUE10TGFIZW+CIAGICAGIDWVYNBTMRPOKJQTU5FZG
DLPGOGICAGICA8YNTBTMRPOKJQTU5FZGDLIGLKPSJGBG93XZF1NWRLCHNFZGKIIGJWBW5FBGVTZW50PSJGBG93XZF1NWRLCHMIPGOGICAGI
CAGIDKATP3YXLWB2LUDCB4PSI30TUIIHK9IJK4MCIGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IOTM1IIB5PSI50DAIIC8+CIAGICA
GICAGPGJWBW5KATPCUE10TGFIZW+CIAGICAGICAGICA8ZG6M91BMRZIHG9IJJ0MSIGET0IOTYIIB3AWR0AD0IMTGIIGHLAWDODD0IM
TQIIC8+CIAGICAGICAGPC9ICG1UZGK6QLBNTKXHYMVSPGOGICAGICA8L2JWBW5KATPCUE10RWRNZT4KICAGICAGPGJWBW5KATPCUE10RWR
NZSBPZD0IRMXVD18WEW83EDEX2RPIIBICG1URWXLBWVUDD0IRMXVD18WEW83EDEXI1J4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0INJYWI
IB5PSI50DAIIC8+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJC0NSIGET0IOTGWIIVPGOGICAGICA8L2JWBW5KATPCUE10RWRNZT4KICA
GICAGPGJWBW5KATPCUE10RWRNZSBPZD0IRMXVD18XCHMXCZLVX2RPIIBICG1URWXLBWVUDD0IRMXVD18XCHMXCZLVJ1J4KICAGICAGICA8Z
GK6D2F5CG9PBNQGED0INDK1IIB5PSI50DAIIC8+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJJ2MCIGET0IOTGWIIVPGOGICAGICA8L2J
WBW5KATPCUE10RWRNZT4KICAGICAGPGJWBW5KATPCUE10RWRNZSBPZD0IRMXVD18XB0TQYCW5Z2RPIIBICG1URWXLBWVUDD0IRMXVD18XB
0TQYCW5Z1J4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IMZYWIIB5PSI50DAIIC8+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJJ0NSIGET0
IOTGWIIVPGOGICAGICA8L2JWBW5KATPCUE10RWRNZT4KICAGICAGPGJWBW5KATPCUE10RWRNZSBPZD0IRMXVD18XCDJ20HNIIJ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IMJA4IIB5PSI50DAIIC8+CIAGICAGICAGPGRPON
DEXBVAW50IHG9IJJ2MCIGET0IOTGWIIVPGOGICAGICA8L2JWBW5KATPCUE10RWRNZT4KICAGICAGPGJWBW5KATPCUE10RWRNZSBPZD0IR
MXVD18XCDPA3ZJX2RPIIBICG1URWXLBWVUDD0IRMXVD18XCDPA3ZJ1J4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IMTMZMCIGET0INJU
YIIVPGOGICAGICAGIDKATP3YXLWB2LUDCB4PSIXMZMIIIB5PSI3MDAIIIC8+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJE0NDI1HK9I
JCWMCIGLZ4KICAGICAGICA8YNTBTMRPOKJQTU5MYWJLBD4KICAGICAGICAGIDKXYPCB3VUZHMGED0IMTMZOCIGET0INJ3Z1IIB3AWR0AD0
IMTUIIGHLAWDODD0IMTQIIC8+CIAGICAGICAGPC9ICG1UZGK6QLBNTKXHYMVSPGOGICAGICA8L2JWBW5KATPCUE10RWRNZT4KICAGICAGP
GJWBW5KATPCUE10RWRNZSBPZD0IRMXVD18XME50GTLX2RPIIBICG1URWXLBWVUDD0IRMXVD18XME50GTL1J4KICAGICAGICA8ZGK6D2F
5CG9PBNQGED0IMTEYNSIGET0INJ3IIVPGOGICAGICAGIDKATP3YXLWB2LUDCB4PSIXMTUWIIB5PSI2MJCIIC8+CIAGICAGIDWVYNBTB
MRPOKJQTU5FZGDLPGOGICAGICA8YNTBTMRPOKJQTU5FZGDLIGLKPSJGBG93XZFWNGSYOTJFZGKIIGJWBW5FBGVTZW50PSJGBG93XZFWNGS
YOTIIPGOGICAGICAGIDKATP3YXLWB2LUDCB4PSIXMZU1IIB5PSI2MJCIIC8+CIAGICAGICAGPGRPONDEXBVAW50IHG9IJE0MTAIIHK9I
JYNYIIGLZ4KICAGICAGICA8YNTBTMRPOKJQTU5MYWJLBD4KICAGICAGICAGIDKXYPCB3VUZHMGED0IMTM3NCIGET0INJA5IIB3AWR0AD0



IMTGTIGIHLAWDODD0IMTQIIC8+CIAGICAGICAGCP9ICG1UZGK6QLBNTKXHYMVSPOGICAGICA8L2JBWB5KATPCUE10RWRNZT4KICAGICAGP
GJWBW5KATPCUE10RWRNZSBPZD0IRMVXD18WYTFPB3N6X2RPIIBICG1URWLWBWUDD0IRMVXD18WYTFPB3N6I1J4KICAGICAGIC8ZGK6D2F
5CG9PBNQGED0IMT1MCIGET0IODIWI1IAPVPOGICAGICAGIDXKATP3YXLWB2LUDCB4PSIXMZEWIIB5PSI4MJAIIIC8+CIAGICAGICAGPGRPO
NDHEXBVAW50IHG9IJEZMTAIHK9IJYZMIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGICAGICG1UZGK6QLBNTKVKZ2UGAWQ
9IKZ5B3DFMTKZZXLS19KASIGYNTBKVSWZ1LBNQ9IKZ5B3DFMTKZZXLS1VY+CIAGICAGICAGPGRPNDDHEXBVAW50IHG9IJEYNTAIHK9I
JYNYVIGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IMTMWNSIGET0INJ1I3I1IAPVPOGICAGICA8L2JBWBW5KATPCUE10RWRNZT4KICAGICA
GPGJWBW5KATPCUE10RWRNZSBPZD0IRMVXD18XDJLMLNLPX2RPIIBICG1URWLWBWUDD0IRMVXD18XDJLMLNPIJ4KICAGICAGICA8ZGK6D
2F5CG9PBNQGED0INJM1IIB5PSI4MJAIIIC8+CIAGICAGICAGPGRPNDDHEXBVAW50IHG9IJEYNTAIHK9IJGYMCIGLZ4KICAGICAGCP9ICG1
UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZGK6QLBNTKVKZ2UGAWQ9IKZ5B3DFMDHUBGR1A19KASIGYNTBKVSWZ1LBNQ9IKZ5B3DFMDHUB
GR1AYI+CIAGICAGICAGPGRPNDDHEXBVAW50IHG9IJIUYMCIGET0IODIWI1IAPVPOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI10DIUHK9IJG
YMCIGLZ4KICAGICAGCP9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZGK6QLBNTKVKZ2UGAWQ9TKZ5B3DFMWP2EXFUYL9KASIGYNTB
KVSZWL1BNQ9IKZ5B3DFMWP2EXFUYL+CIAGICAGICAGPGRPNDDHEXBVAW50IHG9IJM2MCIGET0IODIWI1IAPVPOGICAGICAGIDXKATP3YX
WB2LUDCB4PSI0MJAIIHK9IJIUYMCIGLZ4KICAGICAGCP9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZGK6QLBNTKVKZ2UGAWQ9IKZ5B
3DFMTN3ZNMWOF9KASIGYNTBKVSWZ1LBNQ9IKZ5B3DFMTN3ZNMWOCI+CIAGICAGICAGPGRPNDDHEXBVAW50IHG9IJIWOCIGET0IODIWI1
VPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSIYNJAIHK9IJGYMCIGLZ4KICAGICAGCP9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZ
G6QLBNTKVKZ2UGAWQ9IKZ5B3DFMDQ0BZJY19KASIGYNTBKVSWZ1LBNQ9IKZ5B3DFMDQ0BZJYZI+CIAGICAGICAGPGRPNDDHEXBVAW5
0IHG9IJEYNTAIHK9IJIYNYVIGLZ4KICAGICAGICAG8ZGK6D2F5CG9PBNQGED0IMTA3NSIGET0INJ1I3I1IAPVPOGICAGICA8L2JBWBW5KATPCU
E10RWRNZT4KICAGICAGPGJWBW5KATPCUE10RWRNZSBPZD0IRMVXD18WCMX5NJBXS2RPIIBICG1URWLWBWUDD0IRMVXD18WCMX5NJB5I1J4
KICAGICAGICA8ZGK6D2F5CG9PBNQGED0INJMWIIB5PSI2NTI1IIC8+CIAGICAGICAGPGRPNDDHEXBVAW50IHG9IJIYMCIGET0INZEWI1IAP
GOGICAGICAGIDXKATP3YXLWB2LUDCB4PSIXMDAWIIB5PSI3MTAIIIC8+CIAGICAGICAGPGRPNDDHEXBVAW50IHG9IJEYMDAIHK9IJIY2NYI
GLZ4KICAGICAGCP9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGIDXCIG1UZGK6QLBNTKVKZ2UGAWQ9TKZ5B3DFM9ZAJNVAL9KASIGYNTBKVSWZ
W1LBNQ9IKZ5B3DFMG9ZAJNVAI+CIAGICAGICAGPGRPNDDHEXBVAW50IHG9IJK3NSIGET0INDUWI1IAPVPOGICAGICAGIDXKATP3YXLWB2L
UDCB4PSIXMTUWIIB5PSI0NTAIIIC8+CIAGICAGIDWVYNTBMRPOKJQTU5FZGDLPGOGICAGICA8YNTBMRPOKJQTU5FZGDLIGLKPSJGBG93X
ZA1CMFLNHHFZGKIIGJWBW5FBGVTZW50PSJGBG93XZA1CMFLNHAIPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI5NTAIIHK9IJJQ3NSIGLZ4
KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IOTUWIIB5PSI1MTAIIIC8+CIAGICAGICAGPGRPNDDHEXBVAW50IHG9IJEYMDTIIHK9IJIUXMCIGL
Z4KICAGICAGICA8YNTBMRPOKJQTU5MYWJLB4KICAGICAGICAGIDXKYPCB3VUZHMGED0IOTUWIIB5PSI0TAAIHPDZHROPXSINIGAGV
PZ2H0PSIXNCIGLZ4KICAGICAGICA8L2JBWBW5KATPCUE10TGFIZW+CIAGICAGIDWVYNTBMRPOKJQTU5FZGDLPGOGICAGICA8YNTBMRPO
KJQTU5FZGDLIGLKPSJGBG93XZF5SXA3NTLFZGKIIGJWBW5FBGVTZW50PSJGBG93XZF5SXA3NTKIPGOGICAGICAGIDXKATP3YXLWB2LUDCB
4PSI4NDAAIHK9IJIYNYVIGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IOTMWIIB5PSI2MJCIIIC8+CIAGICAGICAGPGRPNDDHEXBVAW50I
HG9IJKZMCIGET0INDU1I1IAPVPOGICAGICA8L2JBWBW5KATPCUE10RWRNZT4KICAGICAGPGJWBW5KATPCUE10RWRNZSBPZD0IRMVXD18WCZE
XCXKYX2RPIIBICG1URWLWBWUDD0IRMVXD18WCZEXCXYI1J4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0I0DQWIIB5PSI0NTAIIIC8+CIAGI
CAGICAGPGRPNDDHEXBVAW50IHG9IJKYNSIGET0INDUWI1IAPVPOGICAGICA8L2JBWBW5KATPCUE10RWRNZT4KICAGICAGPGRPNDDHEXBVAW50IHG9I
0RWRNZSBPZD0IRMVXD18XMXJ4EDFLJ2RPIIBICG1URWLWBWUDD0IRMVXD18XMXJ4EDFLJ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IN
JU1IIB5PSI2MJCIIIC8+CIAGICAGICAGPGRPNDDHEXBVAW50IHG9IJC0MCIGET0INJ1I3I1IAPVPOGICAGICA8L2JBWBW5KATPCUE10RWRNZT4
KICAGICAGPGJWBW5KATPCUE10RWRNZSBPZD0IRMVXD18WD2DLZNG5X2RPIIBICG1URWLWBWUDD0IRMVXD18WD2DLZNG5I1J4KICAGICAGI
CA8ZGK6D2F5CG9PBNQGED0INDY1IIB5PSI2MJCIIIC8+CIAGICAGICAGPGRPNDDHEXBVAW50IHG9IJIYNSIGET0INJ1I3I1IAPVPOGICAGICA
8L2JBWBW5KATPCUE10RWRNZT4KICAGICAGPGJWBW5KATPCUE10RWRNZSBPZD0IRMVXD18XDH05ZZ3X2RPIIBICG1URWLWBWUDD0IRMVXD
18XDH05ZZ3I1J4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0INDQWIIB5PSI2NTI1IIC8+CIAGICAGICAGPGRPNDDHEXBVAW50IHG9IJC0MC
IGET0INZEWI1IAPVPOGICAGIDXKATP3YXLWB2LUDCB4PSI1MJ1IHK9IJCXMCIGLZ4KICAGICAGICA8YNTBMRPOKJQTU5MYWJLB4KIC
CAGICAGIDXCIXYPCB3VUZHMGED0INDQ4IIB5PSI2NZGI1HDPZHROPXSINISIGAGVPZ2H0PSIXNCIGLZ4KICAGICAGICA8L2JBWBW5KATP
CUE10TGFIZW+CIAGICAGIDWVYNTBMRPOKJQTU5FZGDLPGOGICAGICA8YNTBMRPOKJQTU5FZGDLIGLKPSJGBG93XZE0Y3DLMMSFZGKII
GJWBW5FBGVTZW50PSJGBG93XZE0Y3DLMMAIPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI2NJAIHK9IJIYNYVIGLZ4KICAGICAGICA8ZGK
6D2F5CG9PBNQGED0INDE1IIB5PSI2MJCIIIC8+CIAGICAGIDWVYNTBMRPOKJQTU5FZGDLPGOGICAGICA8YNTBMRPOKJQTU5FZGDLIGLK
PSJGBG93XZE0ZMDXN3FFZGKIIGJWBW5FBGVTZW50PSJGBG93XZE0ZMDXN3EIPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI2NTUIHK9IJJ
1MCTGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0INZQWIIB5PSI0NTAIIIC8+CIAGICAGICAGIDWVYNTBMRPOKJQTU5FZGDLPGOGICAGICA8Y
NTBMRPOKJQTU5FZGDLIGLKPSJGBG93XBZ62GWANRFZGKIIGJWBW5FBGVTZW50PSJGBG93XBZ62WANQIPGOGICAGICAGIDXKATP3YX
WB2LUDCB4PSI2NJAIHK9IJI1MCTGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0INJA1IIB5PSI0NTAIIIC8+CIAGICAGIDWVYNTBMRPO
KJQTU5FZGDLPGOGICAGICA8YNTBMRPOKJQTU5FZGDLIGLKPSJGBG93XBZ6NTIWMZLFZGKIIGJWBW5FBGVTZW50PSJGBG93XBZ6NTIWMZ
IPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSIYMDGI1HK9IJIYNYVIGLZ4KICAGICAGICA8ZGK6D2F5CG9PBNQGED0IMJYWIIB5PSI2MJCII
C8+CIAGICAGIDWVYNTBMRPOKJQTU5FZGDLPGOGICAGICA8YNTBMRPOKJQTU5FZGDLIGLKPSJGBG93XZFYDTCWZGHFZGKIIGJWBW5FBG
VTZW50PSJGBG93XZFYDTCWZGIPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSI2NZUIHK9IJE3MCIGLZ4KICAGICAGICA8ZGK6D2F5CG9P
BNQGED0INZUWIIB5PSIXNZAIIIC8+CIAGICAGICAGPGJWBW5KATPCUE10TGFIZW+CIAGICAGICAGICA8ZGM6QM91BMRZIHG9IJIY40SIGET0
IMTUZIIB3AWR0AD0IM3MIIHLAWDODD0IMTQIIC8+CIAGICAGICAGCP9ICG1UZGK6QLBNTKXHYMVSPOGICAGICA8L2JBWBW5KATPCUE10R
WRNZT4KICAGICAGPGJWBW5KATPCUE10RWRNZSBPZD0IRMVXD18WADH4M3P0X2RPIIBICG1URWLWBWUDD0IRMVXD18WADH4M3P0I1J4KICA
GICAGICA8ZGK6D2F5CG9PBNQGED0INJMWIIB5PSI2MTAIIIC8+CIAGICAGICAGPGRPNDDHEXBVAW50IHG9IJIY2MCIGET0IMT1I1IAPVPOGI
CAGICA8L2JBWBW5KATPCUE10RWRNZT4KICAGICAGPGJWBW5KATPCUE10RWRNZSBPZD0IRMVXD18XCMNSENBOX2RPIIBICG1URWLWBWUDD0
IRMVXD18XCMNSENBOI1J4KICAG

XNZAIIC8+CIAGICAGIDWVYNTBMRPOKJQTU5FZGDLPGOGICAGICA8YNTBMRPOKJQTU5FZGDLIGLKPSJGBG93XE3ANJUN3PFZGKIIGJWB
W5FBGVTZW50PSJGBG93XE3ANJUN30IPGOGICAGICAGIDXKATP3YXLWB2LUDCB4PSIYMDGIH9IJE3MCIGLZ4KICAGICAGICA8ZG6D2F
5CG9PBNQGED0IMJUWIB5PSIXNZAIIC8+CIAGICAGIDWVYNTBMRPOKJQTU5FZGDLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZD0IR
XZLBNRFMXC1AXFRNL9KASIGYNTBKVSWZ1LBNQ9ILN0YXJ0RXZLBNRFMSIGYMLVYZPDHJVA2U9INJNYIG2NYWGMTYWLCA3MSKIIIGJPB2M
6ZMLSBD0ICMDIKDIWMCWGMJMWLCAYMDEPIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJE3MIIGET0IMTUUIB3AWR0AD0IMZYIIGHLAWDOD
D0IMZYIIC8+CIAGICAGICAGPGJWBW5KATPCUE10TGFIZWW+CIAGICAGICAGICA8ZGM6QM91BMRZIHG9IJE10CIGET0IMTK1IIB3AWR0AD0
INJUIIGHLAWDODD0INDAIIC8+CIAGICAGICAGPC9ICG1UZGK6QLBNTKXHYMVSPOGICAGICA8L2JWBW5KATPCUE10U2HHCGU+CIAGICAGI
DXICG1UZGK6QLBNTLNOYXBLIGLKPSJFDMVUDF8XNDRYNNPQX2RPIIBICG1URWXLBWVUDD0IRXZLBNRFMTQ0CJ26AIIIGYMLVYZPDHJVA2U
9INJNYIG2NYWGMTYWLCA3MSKIIIGJPB2M6ZMLSBD0ICMDIKDIWMCWGMJMWLCAYMDEPIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJE3MIIGET
T0INJA5IIB3AWR0AD0IMZYIIGHLAWDODD0IMZYIIC8+CIAGICAGICAGPGJWBW5KATPCUE10TGFIZWW+CIAGICAGICAGICA8ZGM6QM91BMR
ZIHG9IJE1NCIGET0INJUYIIB3AWR0AD0INZQIIGHLAWDODD0IMJCIIC8+CIAGICAGICAGPC9ICG1UZGK6QLBNTKXHYMVSPOGICAGICA8L
2JWBW5KATPCUE10U2HHCGU+CIAGICAGIDXICG1UZGK6QLBNTLNOYXBLIGLKPSJFDMVUDF8XNZBXBXHQX2RPIIBICG1URWXLBWVUDD0IRXZ
LBNRFMTMWCXW0SIGYMLVYZPDHJVA2U9INJNYIG2NYWGMTYWLCA3MSKIIIGJPB2M6ZMLSBD0ICMDIKDIWMCWGMJMWLCAYMDEPIJ4KICAGI
CAGICA8ZGM6QM91BMRZIHG9IJE3MIIGET0INDMYIIB3AWR0AD0IMZYIIGHLAWDODD0IMZYIIC8+CIAGICAGICAGPGJWBW5KATPCUE10TGF
IZWW+CIAGICAGICAGICA8ZGM6QM91BMRZIHG9IJE10CIGET0INDC1IIB3AWR0AD0INJUIIGHLAWDODD0INDAIIC8+CIAGICAGICAGPC9IC
G1UZGK6QLBNTKXHYMVSPOGICAGICA8L2JWBW5KATPCUE10U2HHCGU+CIAGICAGIDXICG1UZGK6QLBNTLNOYXBLIGLKPSJFDMVUDF8XCHA
4A2DYX2RPIIBICG1URWXLBWVUDD0IRXZLBNRFMXBWOGTNCIIGYMLVYZPDHJVA2U9INJNYIG2NYWGMTYWLCA3MSKIIIGJPB2M6ZMLSBD0IC
MDIKDIWMCWGMJMWLCAYMDEPIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJE3MIIGET0I0DAYIIB3AWR0AD0IMZYIIGHLAWDODD0IMZYIIC8
+CIAGICAGICAGPGJWBW5KATPCUE10TGFIZWW+CIAGICAGICAGICA8ZGM6QM91BMRZIHG9IJE10SIGET0I0DQ1IIB3AWR0AD0INJUIIGHL
AWDODD0IMJCIIC8+CIAGICAGICAGPC9ICG1UZGK6QLBNTKXHYMVSPOGICAGICA8L2JWBW5KATPCUE10U2HHCGU+CIAGICAGIDXICG1UZGK
6QLBNTLNOYXBLIGLKPSJFDMVUDF8WBGF2YKX2RPIIBICG1URWXLBWVUDD0IRXZLBNRFMXGHDMM5SIGYMLVYZPDHJVA2U9INJNYIG2N
YWGMTYWLCA3MSKIIIGJPB2M6ZMLSBD0ICMDIKDIWMCWGMJMWLCAYMDEPIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJE3MIIGET0IMT13MI
GD2LKDGG9IJM2IIB0ZWLNAHQ9IJM2IIAVPGOGICAGICAGIDXICG1UZGK6QLBNTKXHYMVSPOGICAGICAGICAGPGR30KJVDW5KCYB4PSIXN
TGIH9IJEZMTUIIHDPZHR0PSI2NYIGAGVPZ2H0PSIXNIGLZ4KICAGICAGICA8L2JWBW5KATPCUE10TGFIZWW+CIAGICAGIDWVYNTBMR
POKJQTU5TAGFWZT4KICAGICAGPGJWBW5KATPCUE10U2HHCGUGAWQ9IKV2ZW50XZFYN3K4DJHFZGKIIGJWBW5FBGVTZW50PSJFDMVUDF8XC
JD50HY4IIBIAW9JONN0CM9RZT0ICMDIKDY3LCAXNJASIDCXKSIGYMLVYZPMAWXSJY2IOMJAWLCAYMZASIDIWMSKIPGOGICAGICAGIDX
KYZPCB3VUZHMGE00IMTGYIIB5PSIYMDGYIIB3AWR0AD0IMZYIIGHLAWDODD0IMZYIIC8+CIAGICAGICAGPGJWBW5KATPCUE10TGFIZWW+C
IAGICAGICAGICA8ZGM6QM91BMRZIHG9IJE30SIGET0IMJEYNSIGD2LKDGG9IJJ3IIB0ZWLNAHQ9IJE0IIAVPGOGICAGICAGIDWVYNTBMR
POKJQTU5MYWJLBD4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZD0IQW0AXZPDHLMFYWMY
2GXB19KASIGYNTBKVSWZ1LBNQ9IKFJDGL2AXR5XZB0XBOY20IPGOGICAGICAGIDXKYZPCB3VUZHMGE00IMJUIIB5PSIXMZAIIHDPZHR
OPSIXMDAIIIGHLAWDODD0I0DAIIC8+CIAGICAGIDWVYNTBMRPOKJQTU5TAGFWZT4KICAGICAGPGJWBW5KATPCUE10U2HHCGUGAWQ9IKFJD
GL2AXR5XZBWDG5MZDFZGKIIGJWBW5FBGVTZW50PSJBY3RPDML0EV8WCHR30TM3IJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJJ4MCIGET0
IMTMWIIIB3AWR0AD0IMTAWIIB0ZWLNAHQ9IJJGWIIVPGOGICAGICA8L2JWBW5KATPCUE10U2HHCGU+CIAGICAGIDXICG1UZGK6QLBNTLNOY
XBLIGLKPSJBY3RPDML0EV8XCHWRZC2J2X2RPIIBICG1URWXLBWVUDD0IRXZLBNRFMTQ0CJ26AIIIGYMLVYZPDHJVA2U9INJNYIG2NYWGMTY
4PSIYNJAIH9IJJQXMCIGD2LKDGG9IJEWMCIAGVPZ2H0PSI4MCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNTB
MRPOKJQTU5TAGFWZSBPZD0IR2F0ZXDHEV8XN2ZMC3HLX2RPIIBICG1URWXLBWVUDD0IR2F0ZXDHEV8XN2ZMC3HLIIBPC01HCTMLCLZPC2L
IBGU9INRYDWUIPGOGICAGICAGIDXKYZPCB3VUZHMGE00INJIIIB5PSIXNDUIIHDPZHR0PSI1MCIGAGVPZ2H0PSI1MCIGLZ4KICAGICAGI
CA8YNTBMRPOKJQTU5MYWJLBD4KICAGICAGICAGIDXKYZPCB3VUZHMGE00INJA4IIB5PSI3NYIGD2LKDGG9IJJGZIIIB0ZWLNAHQ9IJJ2IIA
VPGOGICAGICAGIDWVYNTBMRPOKJQTU5MYWJLBD4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZ
SBPZD0IRXZLBNRFMG04EGR2CL9KASIGYNTBKVSWZ1LBNQ9IKV2ZW50XZBQOHHKDNIIIGJPB2M6C3RYB2TLPSJY2IOMJ15LCA1NYWGNM
PIIBIAW9JOMZPBGW9INJNYIGYNTUSIDIWNSWGMJEKWSI+CIAGICAGICAGPGR30KJVDW5KCYB4PSI30DIIH9IJJYMIIGD2LKDGG9IJM2I
IBOZWLNAHQ9IJM2IIAVPGOGICAGICAGIDXICG1UZGK6QLBNTKXHYMVSPOGICAGICAGICAGPGR30KJVDW5KCYB4PSI30DKIIH9IJJ2NSI
GD2LKDGG9IJJ2IIB0ZWLNAHQ9IJE0IIAVPGOGICAGICAGIDWVYNTBMRPOKJQTU5MYWJLBD4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBL
GOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZD0IR2F0ZXDHEV8WCMJEHAYX2RPIIBICG1URWXLBWVUDD0IR2F0ZXDHEV8XZJM0Y3A0IJ4
KICAGICAGICA8ZGM6QM91BMRZIHG9IJJYWNISIGET0IND1IIB3AWR0AD0INTAIIIGHLAWDODD0INTAIIIC8+CIAGICAGIDWVYNTBMRPOKJQT
U5TAGFWZT4KICAGICAGPGJWBW5KATPCUE10U2HHCGUGAWQ9IKFJDGL2AXR5XZBQ0DYXB1FZGKIIGJWBW5FBGVTZW50PSJBY3RPDML0EV8
WAJG2MW5TIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJJ4MCIGET0IMZEWIIB3AWR0AD0IMTAWIIB0ZWLNAHQ9IJJGWIIVPGOGICAGICA8L
2JWBW5KATPCUE10U2HHCGU+CIAGICAGIDXICG1UZGK6QLBNTLNOYXBLIGLKPSJBY3RPDML0EV8XDHCSAGJ1X2RPIIBICG1URWXLBWVUDD0
IQW0AXZPDHLMXR30WHIDSIGYMLVYZPDHJVA2U9INJNYIGZMCGMTM2LCAYMJKPIIBIAW9JOMZPBGW9INJNYIGXODCSIDIYMIWGMJUXK
SI+CIAGICAGICAGPGR30KJVDW5KCYB4PSI3NTAIIH9IJJZMCIGD2LKDGG9IJEWMCIAGVPZ2H0PSI4MCIGLZ4KICAGICAGPC9ICG1UZGK
6QLBNTLNOYXBLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZD0IQW0AXZPDHLMWZNM6T6DF9KASIGYNTBKVSWZ1LBNQ9IKFJDGL2A
XR5XZFMZEWENQIPGOGICAGICAGIDXKYZPCB3VUZHMGE00IMJYIIB5PSI10DCIIBDPZHR0PSIXMDAIIIGHLAWDODD0I0DAIIC8+CIAGICA
GIDWVYNTBMRPOKJQTU5TAGFWZT4KICAGICAGPGJWBW5KATPCUE10U2HHCGUGAWQ9IKFJDGL2AXR5XZF0Y2N0ANNFZGKIIGJWBW5FBGVTZ
W50PSJBY3RPDML0EV8XDNJDPZIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJC0MCIGET0INDEWIIB3AWR0AD0IMTAWIIB0ZWLNAHQ9IJJG
WIIVPGOGICAGICA8L2JWBW5KATPCUE10U2HHCGU+CIAGICAGIDXICG1UZGK6QLBNTLNOYXBLIGLKPSJHYXRLD2F5XZB50G0XYMJFZGKI
GJWBW5FBGVTZW50PSJHYXRLD2F5XZB50G0XYMIIGLZTWFYA2VYVMLZAWJSZT0IDHJ1ZSI+CIAGICAGICAGPGR30KJVDW5KCYB4PSI0MTU
I1HK9IJJYMMIIGD2LKDGG9IJJYIIB0ZWLNAHQ9IJJUWIIAVPGOGICAGICAGIDXICG1UZGK6QLBNTKXHYMVSPOGICAGICAGICAGPGR30KJVD
W5KCYB4PSIZ0TUIH9IJJYUNYIGD2LKDGG9IJJ5IIB0ZWLNAHQ9IJJY2IIAVPGOGICAGICAGIDWVYNTBMRPOKJQTU5MYWJLBD4KICAGICA
GPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZD0IRXZLBNRFMHRSAH5ZL9KASIGYNTBKVSWZ1LBNQ9I
KV2ZW50XZB0BGH20WYIIGJPB2M6C3RYB2TLPSJY2IOMJ15LCA1NYWGNMTPIIBIAW9JOMZPBGW9INJNYIGYNTUSIDIWNSWGMJEKWSI+CIA
GICAGICAGPGR30KJVDW5KCYB4PSI1MJIIH9IJJY5MIIGD2LKDGG9IJM2IIB0ZWLNAHQ9IJM2IIAVPGOGICAGICAGIDXICG1UZGK6QLBNT
KXHYMVSPOGICAGICAGICAGPGR30KJVDW5KCYB4PSI1MJKI1H9IJJZNSIGD2LKDGG9IJJ2IIB0ZWLNAHQ9IJE0IIAVPGOGICAGICAGIDW
VYNTBMRPOKJQTU5MYWJLBD4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZD0IR2F0ZXDHE
V8WYMYJETHOX2RPIIBICG1URWXLBWVUDD0IR2F0ZXDHEV8XBLMDG14I4KICAGICAGICA8ZGM6QM91BMRZIHG9IJJYWNISIGET0INJAYIIB
3AWR0AD0INTAIIIGHLAWDODD0INTAIIIC8+CIAGICAGIDWVYNTBMRPOKJQTU5TAGFWZT4KICAGICAGPGJWBW5KATPCUE10U2HHCGUGAWQ9I
KFJDGL2AXR5XZE1AXLJB3LJFZGKIIGJWBW5FBGVTZW50PSJBY3RPDML0EV8XNWL5Y24SIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJC0MC
IGET0INTG3IIB3AWR0AD0IMTAWIIB0ZWLNAHQ9IJJGWIIVPGOGICAGICA8L2JWBW5KATPCUE10U2HHCGU+CIAGICAGIDXICG1UZGK6QLBNT
LNOYXBLIGLKPSJHYXRLD2F5XZFRMZHHMNFZGKIIGJWBW5FBGVTZW50PSJHYXRLD2F5XZFRMZHHMNEIIGLZTWFYA2VYVMLZAWJSZT0IDHJ

[illegible]

WBHYIIGLZTWFYA2VYVWMLZAWJSZT0IDHJ1ZSI+CIAGICAGICAGPGRJOKJVDW5KCYB4PSI0MJUIIHK9IJEYNJUIIHDZPHROPSI1MCIGAGVPZ
2H0PS11MCIGLZ4KICAGICAGICA8YNTBMRPOKJQTU5MYWJLBD4KICAGICAGICAGIDKXZPCB3VUZHMGE00INDA2IIB5PSIXMJ1WI1B3AWR
0AD0I0DCIIGHLAWD0DD0INDAIIIC8+CIAGICAGICAGPC9ICG1UZGK6QLBNTKXHYMVSPGOGICAGICA8L2JWBW5KATPCUE10U2HHCUGU+CIAGI
CAGIDXCIG1UZGK6QLBNTLNOYXBLIGLKP5JHYXRLD2F5XZBYNW50CW5FZGKIIGJWBW5FBGVTZW50PSJHYXRLD2F5XZF3BMLTEDUIPGOGICA
GICAGIDKXZPCB3VUZHMGE00INTG1IIB5PSIXMJY1IIB3AWR0AD0INTAIIIGHLAWD0DD0INTAIIIC8+CIAGICAGIDWVYNB1BMRPOKJQTU5TA
GFWZT4KICAGICAGPGJWBW5KATPCUE10U2HHCUGUAWQ9IKV2ZW50XZFJCMV1AMNFZGKIIGJWBW5FBGVTZW50PSJFDMVUDF8XY3JLDWPJ1IB
IAW9JONN0CM9RZT0ICMDIKDIYOSWGNCTSIDUZK5IGYMLVYZPMAWXS5PSJY22IOMJ1L1CAYMDUSIDIXMKIPGOGICAGICAGIDKXZPCB3VUZ
HMGED0INTEYIIB5PSIXMZGYIIB3AWR0AD0IMZYIIGHLAWD0DD0IMZYIIC8+CIAGICAGICAGPGJWBW5KATPCUE10TGFIZWW+CIAGICAGICA
GICA8ZGM6QM91BMRZIHG9IJUXOSIGET0IMTQYNSIGD2LKDGG9IJJIZIIBOZWLNAHQ9IJE0IIAVPGOGICAGICAGIDWVYNB1BMRPOKJQTU5MY
WJLBD4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZD0IQWN0AXZPDHLMFNTVDZHHCL9KASI
GYNTBKVSVZW1LBNQ9IKFJDGL2AXR5XZEZB3C4YXIIIGJPB2M6C3RYB2TLP5JY22IOMZASIDEZNIWGMJ15K5IGYMLVYZPMAWXS5PSJY22IOM
TG3LCAYMJISIDI1MSKIPGOGICAGICAGIDKXZPCB3VUZHMGE00INZUWIIIB5PSIXMZKWIIB3AWR0AD0IMTAWIIBOZWLNAHQ9IJGWI1AVPGO
GICAGICA8L2JWBW5KATPCUE10U2HHCUGU+CIAGICAGIDXCIG1UZGK6QLBNTLNOYXBLIGLKP5JB3Y3RPDML0EV8WM2R0D2SXX2RPIIBICG1UR
WXLBWVUDD0IQWN0AXZPDHLMFMMHMD2D3YIYI+CIAGICAGICAGPGRJOKJVDW5KCYB4PSI3NTAIIHK9IJEYNTAIIHDPZHR0PSIXMDAIIIGHLAWD
0DD0I0DAIIIC8+CIAGICAGIDWVYNB1BMRPOKJQTU5TAGFWZT4KICAGICAGPGJWBW5KATPCUE10U2HHCUGUAWQ9IKFJDGL2AXR5XZB0NWHQ0
WZFZGKIIGJWBW5FBGVTZW50PSJB3Y3RPDML0EV8WDDVOAJLMJ14KICAGICAGICA8ZGM6QM91BMRZIHG9IJK1MCIGET0IMT11MCIGD2LKDGG
9IJEWMCIAGAGVPZ2H0PSI4MCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZD0IR2F0Z
XDHEV8WN2J0ZXJXX2RPIIBICG1URWXLBWVUDD0IR2F0ZXDHEV8WN2J0ZXJJIIBPC0IHCMTLCLZPC2LIBG9INRYDUUIPGOGICAGICAGIDX
KYZPCB3VUZHMGE00IMTE1NSIGET0IMTI2NSIGD2LKDGG9IJJUWIIIBOZWLNAHQ9IJJUWIIAVPGOGICAGICAGIDXCIG1UZGK6QLBNTKXHYMVSP
GOGICAGICAGICAGPGRJOKJVDW5KCYB4PSIXMTM5IIB5PSIXMZMWIIB3AWR0AD0I0DIIIGHLAWD0DD0INDAIIIC8+CIAGICAGICAGPC9ICG1
UZGK6QLBNTKXHYMVSPGOGICAGICA8L2JWBW5KATPCUE10U2HHCUGU+CIAGICAGIDXCIG1UZGK6QLBNTLNOYXBLIGLKP5JB3Y3RPDML0EV8XC
NDYBTH5X2RPIIBICG1URWXLBWVUDD0IQWN0AXZPDHLMFXJ3CM04ESIGYMLVYZPDHJVA2U9INJNYIGZMCGMTM2LCAYMJKPIIBIAW9JOMZ
PBGW9INJNYIGXODCSIDIYMIWGMJUXKSI+CIAGICAGICAGPGRJOKJVDW5KCYB4PSIXNDAWIIB5PSIXMJUWIIIB3AWR0AD0IMTAWIIBOZWLNA
HQ9IJGWI1AVPGOGICAGICA8L2JWBW5KATPCUE10U2HHCUGU+CIAGICAGIDXCIG1UZGK6QLBNTLNOYXBLIGLKP5JB3Y3RPDML0EV8WANPNBXD
QX2RPIIBICG1URWXLBWVUDD0IQWN0AXZPDHLMFGP6Z21AI+CIAGICAGICAGPGRJOKJVDW5KCYB4PSIXNDWIIB5PSIXMZMWIIB3AWR0AD0IMTAWIIBOZWLNA
SIXMDAIIIGHLAWD0DD0I0DAIIIC8+CIAGICAGIDWVYNB1BMRPOKJQTU5TAGFWZT4KICAGICAGPGJWBW5KATPCUE10U2HHCUGUAWQ9IKFJDGL
2AXR5XZFYANHYNGVFZGKIIGJWBW5FBGVTZW50PSJB3Y3RPDML0EV8XCMPC43RLIIBIAW9JONN0CM9RZT0ICMDIKDMWLCAWMZYSIDIYOSKII
GJPB2M6ZMLSD0ICMDIKDE4NYWGMJ1YLCAYNTEPIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJK5MCIGET0IMJ4MCIGD2LKDGG9IJEWMCI
AGVPZ2H0PSI4MCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZD0IR2F0ZXDHEV8WC
2ZMZM00X2RPIIBICG1URWXLBWVUDD0IR2F0ZXDHEV8WC2X6MJL1J14KICAGICAGICA8ZGM6QM91BMRZIHG9IJJUWIIIBOZWLNAHQ9IJJUWII
KDGG9IJJUWIIIBOZWLNAHQ9IJJUWIIAVPGOGICAGICA8L2JWBW5KATPCUE10U2HHCUGU+CIAGICAGIDXCIG1UZGK6QLBNTLNOYXBLIGLKP5JB
3Y3RPDML0EV8WANZHNG3VX2RPIIBICG1URWXLBWVUDD0IQWN0AXZPDHLMFGP2YTRIBYI+CIAGICAGICAGPGRJOKJVDW5KCYB4PSI2MDAIIHK
9IJI0T0AIIHDPZHR0PSIXMDAIIIGHLAWD0DD0I0DAIIIC8+CIAGICAGIDWVYNB1BMRPOKJQTU5TAGFWZT4KICAGICAGPGJWBW5KATPCUE10U
2HHCUGUAWQ9IKDHDGV3YXLFMWDS2RUYL9KASIGYNTBKVSVZW1LBNQ9IKFJDGL2AXR5XZB5AZG2EYWIIGJPB2M6C3RYB2TLP5JY22IOMZASIDEZNIW
LIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJE0TUIIHK9IJJIMDUIIHDZPHROPSI1MCIGAGVPZ2H0PSI1MCIGLZ4KICAGICAGICA8YNTB
MRPOKJQTU5MYWJLBD4KICAGICAGICAGIDKXZPCB3VUZHMGE00IMTE30CIGET0IMJQ1MYIGD2LKDGG9IJJ0IIBOZWLNAHQ9IJJUZI1AVPGO
GICAGICAGIDWVYNB1BMRPOKJQTU5MYWJLBD4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZ
D0IQWN0AXZPDHLMFXRODZ5ZL9KASIGYNTBKVSVZW1LBNQ9IKFJDGL2AXR5XZB5AZG2EYWIIGJPB2M6C3RYB2TLP5JY22IOMZASIDEZNIW
GMJ15K5IGYMLVYZPMAWXS5PSJY22IOMTG3LCAYMJISIDI1MSKIPGOGICAGICAGIDKXZPCB3VUZHMGE00IMT0MCIGET0IMJQ5MCIGD2LKD
GG9IJEWMCIAGAGVPZ2H0PSI4MCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZD0IRXZ
LBNRFMHBJA200DV9KASIGYNTBKVSVZW1LBNQ9IKV2ZW50XZBWY2TQNHUIIGJPB2M6C3RYB2TLP5JY22IOMJ15LCA1NYWGNTPM1IBIAW9J0
MZPBGW9INJNYIGYNTUSIDIWNSWGMJEWSI+CIAGICAGICAGPGRJOKJVDW5KCYB4PSIXMJGYIIB5PSIYNTKYIIB3AWR0AD0IMZYIIGHLAWD
0DD0IMZYIIC8+CIAGICAGICAGPGJWBW5KATPCUE10TGFIZWW+CIAGICAGICAGICA8ZGM6QM91BMRZIHG9IJEYODKIHK9IJJ1ZMZUIIHDZ
HROPSIYMYIAGAGVPZ2H0PSIXNCIGLZ4KICAGICAGICA8L2JWBW5KATPCUE10TGFIZWW+CIAGICAGIDWVYNB1BMRPOKJQTU5TAGFWZT4KICA
GICAGPGJWBW5KATPCUE10U2HHCUGUAWQ9IKFJDGL2AXR5XZAZDDJXOHRFZGKIIGJWBW5FBGVTZW50PSJB3Y3RPDML0EV8WM3QYCTH0IJ4KI
CAGICAGICA8ZGM6QM91BMRZIHG9IJJ5MCIGET0IMJ2MCIGD2LKDGG9IJEWMCIAGAGVPZ2H0PSI4MCIGLZ4KICAGICAGPC9ICG1UZGK6QLB
NTLNOYXBLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZD0IR2F0ZXDHEV8WMHKKZEHLX2RPIIBICG1URWXLBWVUDD0IR2F0ZXDHEV8XZ
GZ3C2MXIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJJUYNISIGET0IMJ3DNEISIGD2LKDGG9IJJUWIIIBOZWLNAHQ9IJJUWIIAVPGOGICAGICA8L2J
WBW5KATPCUE10U2HHCUGU+CIAGICAGIDXCIG1UZGK6QLBNTLNOYXBLIGLKP5JB3Y3RPDML0EV8XCM5WOGG4X2RPIIBICG1URWXLBWVUDD0IQ
WN0AXZPDHLMFXJUCDH0OCIGYMLVYZPDHJVA2U9INJNYIGZMCGMTM2LCAYMJKPIIBIAW9JOMZPBGW9INJNYIGXODCSIDIYMIWGMJUXKSI
+CIAGICAGICAGPGRJOKJVDW5KCYB4PSI30T0AIIHK9IJJUWIIHDPZHR0PSIXMDAIIIGHLAWD0DD0I0DAIIIC8+CIAGICAGIDWVYNB1BMRPO
KJQTU5TAGFWZT4KICAGICAGPGJWBW5KATPCUE10U2HHCUGUAWQ9IKFJDGL2AXR5XZFYMHSAVFXZGKIIGJWBW5FBGVTZW50PSJB3Y3RPDML
0EV8XCWJ0BGL1IJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJJYZMCIGET0IMJ3E3MCIGD2LKDGG9IJEWMCIAGAGVPZ2H0PSI4MCIGLZ4KICAGI
CAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZD0IR2F0ZXDHEV8WDBQMDJRX2RPIIBICG1URWXLBWV
UDD0IR2F0ZXDHEV8WDBQMDJRIIBPC0IHCMTLCLZPC2LIBG9INRYDUUIPGOGICAGICAGIDKXZPCB3VUZHMGE00IMTE2NSIGET0IMJE4N
SIGD2LKDGG9IJJUWIIIBOZWLNAHQ9IJJUWIIAVPGOGICAGICAGIDXCIG1UZGK6QLBNTKXHYMVSPGOGICAGICAGPGRJOKJVDW5KCYB4PSI
XMTUYIIB5PSIYMTA3IIB3AWR0AD0INZYIIGHLAWD0DD0INZYIIC8+CIAGICAGICAGPC9ICG1UZGK6QLBNTKXHYMVSPGOGICAGICA8L2JWB
W5KATPCUE10U2HHCUGU+CIAGICAGIDXCIG1UZGK6QLBNTLNOYXBLIGLKP5JB3Y3RPDML0EV8XZRLBGI0X2RPIIBICG1URWXLBWVUDD0IQWN
0AXZPDHLMFMMV02WXXINCIGYMLVYZPDHJVA2U9INJNYIGZMCGMTM2LCAYMJKPIIBIAW9JOMZPBGW9INJNYIGXODCSIDIYMIWGMJUXKSI+C
IAGICAGICAGPGRJOKJVDW5KCYB4PSIXMZWIIB5PSIYMTCWIIB3AWR0AD0IMTAWIIBOZWLNAHQ9IJJGWI1AVPGOGICAGICA8L2JWBW5KATP
CUE10U2HHCUGU+CIAGICAGIDXCIG1UZGK6QLBNTLNOYXBLIGLKP5JFDMVUDF8XN23DMGWX2RPIIBICG1URWXLBWVUDD0IRXZLBNRFMTDNN
3ZOMCIGYMLVYZPDHJVA2U9INJNYIGYMKJSDU3LCA1MYKIJIGJPB2M6ZMLSD0ICMDIKDI1NSWGMJ1AL1CAYMTAPJ14KICAGICAGICA8ZGM
6QM91BMRZIHG9IJEYNZIIHK9IJJIZMDIIHDPZHR0PSI2NIIGAGVPZ2H0PSI2NIIGLZ4KICAGICAGICA8YNTBMRPOKJQTU5MYWJLBD4KI
CAGICAGICAGIDKXZPCB3VUZHMGE00IMTI30SIGET0IMJ0M0NSIGD2LKDGG9IJJIZIIBOZWLNAHQ9IJE0IIAVPGOGICAGICAGIDWVYNB1BMR
POKJQTU5MYWJLBD4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZD0IQWN0AXZPDHLMFMTD
GHZ0V9KASIGYNTBKVSVZW1LBNQ9IKFJDGL2AXR5XZFPBXROCKZPGOGICAGICAGIDKXZPCB3VUZHMGE00IMJ12MCIGET0IMTAWMCIGD2L
KDGG9IJEWMCIAGAGVPZ2H0PSI4MCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNTBMRPOKJQTU5TAGFWZSBPZD0IR
2F0ZXDHEV8WBWE2YTHOX2RPIIBICG1URWXLBWVUDD0IR2F0ZXDHEV8WCJHYTA5IJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJI0TUIIHK

91JEWMTUIIHPDZHRPSSI1MCIGAGVPZ2H0PSI1MCIGLZ4KICAGICAGICA8YNBTBMRPOKJQTU5MYWJLBD4KICAGICAGICAGIDKXYZPCB3VUZ
HMGED0MTJQXMCIGET0IOTCZIIIB3AWR0AD0INZKIIGHLAWDODD0INTMIIC8+CIAGICAGICAGPC9ICG1UZGK6QLBNTKXHYMVSPOGICAGICA
8L2JWBW5KATPCUE10U2HHCUGU+CIAGICAGIDXCIG1UZGK6QLBNTLNOYXBLIGLKP5JB3RDPML0EV8XN204NDC4X2RPIIBICG1URWXLBWVUD
D0IQWN0AXZPDHLMFTD0DQ30CI+CIAGICAGICAGPGRJOKJVDW5KCYB4PSIYNJGWIIB5PSIXMDAWIIB3AWR0AD0IMTAWIIBOZWLNAHQ9IJG
WIAVPGOGICAGICA8L2JWBW5KATPCUE10U2HHCUGU+CIAGICAGIDXCIG1UZGK6QLBNTLNOYXBLIGLKP5JB3RDPML0EV8XMDBTMXVMX2RPI
IBICG1URWXLBWVUD0IQWN0AXZPDHLMFTAWBT1ZII+CIAGICAGICAGPGRJOKJVDW5KCYB4PSIYNJGWIIB5PSI4NJAIHPDZHRPSSIXMDA
IIGHLAWDODD0I0DAIIC8+CIAGICAGIDWVYNBTBMRPOKJQTU5TAGFWZT4KICAGICAGPGJWBW5KATPCUE10U2HHCUGUAWQ9IKFJ0GL2AXR5X
ZE0CHVQC29FZGKIIGJWBW5FBGVTZ5W0PSJB3RDPML0EV8XNHB1ANNVIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJJ20DAIHHK9IJEJXMA
IHPDZHRPSSIXMDAIIIGHLAWDODD0I0DAIIC8+CIAGICAGIDWVYNBTBMRPOKJQTU5TAGFWZT4KICAGICAGPGJWBW5KATPCUE10U2HHCUGU
WQ9IKFJ0GL2AXR5XZBNZHHMFLZGKIIGJWBW5FBGVTZ5W0PSJB3RDPML0EV8XN3NWDMUZIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJJ
5M3AIHHK9IJEJWMDAIHPDZHRPSSIXMDAIIIGHLAWDODD0I0DAIIC8+CIAGICAGIDWVYNBTBMRPOKJQTU5TAGFWZT4KICAGICAGPGJWBW5KA
TPCUE10U2HHCUGUAWQ9IKV2Z5W0XZBIOXNUCJVFZGKIIGJWBW5FBGVTZ5W0PSJFDMVUDF8WYJLZBNI1IIBIAW9JONN0CM9RZT0ICMDIKDI
YOSWGTCSIDUZKISIGYMLVYZPMAWXSJYZ2IOMJU1LCAYMDSIDIXMKIPGOGICAGICAGIDKXYZPCB3VUZHMGED0MTZE2MIIGET0IMTAYM
IIGD2LKDGG9IJJM2IIBOZWLNAHQ9IJJM2IIAVPGOGICAGICAGIDXCIG1UZGK6QLBNTKXHYMVSPOGICAGICAGPGRJOKJVDW5KCYB4PSI
ZMTY5IIB5PSIXMDYI1IB3AWR0AD0IMJMIIGHLAWDODD0IMTQIIC8+CIAGICAGICAGPC9ICG1UZGK6QLBNTKXHYMVSPOGICAGICA8L2JWB
W5KATPCUE10U2HHCUGU+CIAGICAGIDXCIG1UZGK6QLBNTLNOYXBLIGLKP5JFDMVUDF8WYJLZBNI1IIBICG1URWXLBWVUD0IRXZLBNR
FMHR3EJYYMICYGMLVYZPDHJVA2U9INJNYIG2NYWGMTYWLCA3MSKIIIGJPB2M6ZMLSD0ICMDIKDIWMCWGMJMWLCAYMDEPIJ4KICAGICAGI
CA8ZGM6QM91BMRZIHG9IJE3MIIGET0IMTYZMIIGD2LKDGG9IJJM2IIBOZWLNAHQ9IJJM2IIAVPGOGICAGICAGIDXCIG1UZGK6QLBNTKXHYM
VSPGOGICAGICAGPGRJOKJVDW5KCYB4PSIXNTAIHHK9IJE2NZUIIHPDZHRPSSI4NSIGAGVPZ2H0PSIYNYIGLZ4KICAGICAGICA8L2JWB
W5KATPCUE10TGFIZWW+CIAGICAGIDWVYNBTBMRPOKJQTU5TAGFWZT4KICAGICAGPGJWBW5KATPCUE10U2HHCUGUAWQ9IKFJ0GL2AXR5XZ
XEF6D2ZFZGKIIGJWBW5FBGVTZ5W0PSJB3RDPML0EV8XCLXENDMIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJJ2MCIGET0IMTYXMCIGD
2LKDGG9IJEWMCIAGAGVPZ2H0PSI4MCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNBTBMRPOKJQTU5TAGFWZSBPZD0
IR2F0ZXDHEV8WBZL5D21TX2RPIIBICG1URWXLBWVUD0IR2F0ZXDHEV8XDHE1BZYWIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJJQXNSIGE
T0IMTYNSIGD2LKDGG9IJJWIIIBOZWLNAHQ9IJJWIIIAVPGOGICAGICA8L2JWBW5KATPCUE10U2HHCUGU+CIAGICAGIDXCIG1UZGK6QLBNTL
NOYXBLIGLKP5JB3RDPML0EV8XDDZ0YNPWX2RPIIBICG1URWXLBWVUD0IQWN0AXZPDHLMFHQ2AGJ6CCI+CIAGICAGICAGPGRJOKJVDW5K
YB4PSI1MJAIHHK9IJE2MTAIHPDZHRPSSIXMDAIIIGHLAWDODD0I0DAIIC8+CIAGICAGIDWVYNBTBMRPOKJQTU5TAGFWZT4KICAGICAGPGJ
WBW5KATPCUE10U2HHCUGUAWQ9IKDHDGV3YXLFMT1AWR5C19KASIGYNBTBKVSZW1LBNQ9IKDHDGV3YXLFMT1AWR5CYIGAXNNYX3RZXJWA
XNPYMLPSJ0CNVLIJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJJ3NSIGET0IMTYNSIGD2LKDGG9IJJWIIIBOZWLNAHQ9IJJWIIIAVPGOGICA
GICAGIDXCIG1UZGK6QLBNTKXHYMVSPOGICAGICAGPGRJOKJVDW5KCYB4PSI3MTUIIHHK9IJE1NJCIHPDZHRPSSI40SIGAGVPZ2H0P
SI2NIIGLZ4KICAGICAGICA8L2JWBW5KATPCUE10TGFIZWW+CIAGICAGIDWVYNBTBMRPOKJQTU5TAGFWZT4KICAGICAGPGJWBW5KATPCUE1
0U2HHCUGUAWQ9IKFJ0GL2AXR5XZFXCWNKNW5FZGKIIGJWBW5FBGVTZ5W0PSJB3RDPML0EV8XCFJZDVUIJ4KICAGICAGICA8ZGM6QM91B
MRZIHG9IJJ5MCIIGET0IMTC3MCIIGD2LKDGG9IJEWMCIAGAGVPZ2H0PSI4MCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA
8YNBTBMRPOKJQTU5TAGFWZSBPZD0IQWN0AXZPDHLMFHJ2M2FUCV9KASIGYNBTBKVSZW1LBNQ9IKFJ0GL2AXR5XZBYDJNHBNEIPGOGICAGI
CAGIDKXYZPCB3VUZHMGED0INTYWIIB5PSIXNDYWIIB3AWR0AD0IMTAWIIBOZWLNAHQ9IJJWIIIAVPGOGICAGICA8L2JWBW5KATPCUE10U2H
HCGU+CIAGICAGIDXCIG1UZGK6QLBNTLNOYXBLIGLKP5JB3RDPML0EV8WMMFPMNMTKX2RPIIBICG1URWXLBWVUD0IQWN0AXZPDHLMFDFHA
TZRZCIGYMLVYZPDHJVA2U9IMXZTG4ZTUIIGJPB2M6ZMLSD0II2JIZGVMYIIGY29SB3I6YMFJA2DYB3VUZC1JB2XVCJ0II2JIZGVMYII
GY29SB3I6YMY9ZGVYLWNVBG9YPSIJMWU40GU1IJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJJ2MCIGET0IMTYXMCIGD2LKDGG9IJEWMCI
GAGVPZ2H0PSI4MCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNBTBMRPOKJQTU5TAGFWZSBPZD0IRXZLBNRFTI1Z3D
QYL9KASIGYNBTBKVSZW1LBNQ9IKV2Z5W0XZEYNWD3AMIIGJPB2M6C3RYB2TLPSIJZTUZOTM1IIBIAW9JOMZPBGW9IINXZMMNKZDIIGNVB
G9YOMJHY2TNCM91BMQTY29SB3I9IINMZMKNZDIIGNVBG9YOMJVCMLCI1JB2XVCJ0II2U1MZKZNSI+CIAGICAGICAGPGRJOKJVDW5KCYB
4PSI4NJAIHHK9IJE3MJIIHPDZHRPSSIZNIIGAGVPZ2H0PSI2NIIGLZ4KICAGICAGICA8YNBTBMRPOKJQTU5MYWJLBD4KICAGICAGICAGI
DKXYZPCB3VUZHMGED0I0DY5IIB5PSIXNZYI1IB3AWR0AD0IMJMIIGHLAWDODD0IMTQIIC8+CIAGICAGICAGPC9ICG1UZGK6QLBNTKXHYM
VSPGOGICAGICA8L2JWBW5KATPCUE10U2HHCUGU+CIAGICAGIDXCIG1UZGK6QLBNTLNOYXBLIGLKP5JHYXRLD2F5XZBNETU0DHLFZGKIIGJWB
W5FBGVTZ5W0PSJHYXRLD2F5XZBNETU0DHLFZGKIIGLZTWFYA2VYVYLZAWJSZT0IDHJ1ZSI+CIAGICAGICAGPGRJOKJVDW5KCYB4PSI1NDUIHHK
9IJE30DUIHPDZHRPSSI1MCIGAGVPZ2H0PSI1MCIGLZ4KICAGICAGICA8YNBTBMRPOKJQTU5MYWJLBD4KICAGICAGICAGIDKXYZPCB3VUZ
HMGED0INTM2IIB5PSIXNZQWIIIB3AWR0AD0INJCIIGHLAWDODD0INDAIIC8+CIAGICAGICAGPC9ICG1UZGK6QLBNTKXHYMVSPOGICAGICA
8L2JWBW5KATPCUE10U2HHCUGU+CIAGICAGIDXCIG1UZGK6QLBNTLNOYXBLIGLKP5JB3RDPML0EV8WY2W2NDHL2RPIIBICG1URWXLBWVUD
D0IQWN0AXZPDHLMFGNSJQ4Z9IIGYMLVYZPDHJVA2U9IIMXZTG4ZTUIIGJPB2M6ZMLSD0II2JIZGVMYIIGY29SB3I6YMFJA2DYB3VUZC1
JB2XVCJ0II2JIZGVMYIIGY29SB3I6YMY9ZGVYLWNVBG9YPSIJMWU40GU1IJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJJ1MCIGET0IMTC3M
CIGD2LKDGG9IJEWMCIAGAGVPZ2H0PSI4MCIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTLNOYXBLPGOGICAGICA8YNBTBMRPOKJQTU5TAGFWZSB
PZD0IQWN0AXZPDHLMFGVHZMTUDF9KASIGYNBTBKVSZW1LBNQ9IKFJ0GL2AXR5XZBLWYRBNQIPGOGICAGICAGIDKXYZPCB3VUZHMGED0IN
TAWIIB5PSIXOTQWIIIB3AWR0AD0IMTAWIIBOZWLNAHQ9IJJWIIIAVPGOGICAGICA8L2JWBW5KATPCUE10U2HHCUGU+CIAGICAGIDXCIG1UZGK
6QLBNTLNOYXBLIGLKP5JFDMVUDF8XZXWUNZJ0X2RPIIBICG1URWXLBWVUD0IRXZLBNRFMVSB3CYACIGYMLVYZPDHJVA2U9IINLNTM5M
ZUIIGJPB2M6ZMLSD0II2ZMY2RKMIIGY29SB3I6YMFJA2DYB3VUZC1JB2XVCJ0II2ZMY2RKMIIGY29SB3I6YMY9ZGVYLWNVBG9YPSIJZTU
ZOTM1IJ4KICAGICAGICA8ZGM6QM91BMRZIHG9IJJ1MIIGET0IMTG2MIIGD2LKDGG9IJJM2IIBOZWLNAHQ9IJJM2IIAVPGOGICAGICAGIDXCIG
1UZGK6QLBNTKXHYMVSPOGICAGICAGPGRJOKJVDW5KCYB4PSI2NTKIIHK9IJE5MDUIHPDZHRPSSIYMYIAGAGVPZ2H0PSIXNIGLZ4
KICAGICAGICA8L2JWBW5KATPCUE10TGFIZWW+CIAGICAGIDWVYNBTBMRPOKJQTU5TAGFWZT4KICAGICAGPGJWBW5KATPCUE10U2HHCUGU
WQ9IIRLEHRRBMSVDF0AW9UXZBPNND3MFLZGKIIGJWBW5FBGVTZ5W0PSJUZXH0QW5UB3RHDGLVBL8WATQZDZM5IJ4KICAGICAGICA8ZGM
6QM91BMRZIHG9IJJ1MCIGET0IMJUSNSIGD2LKDGG9IJEWMCIAGAGVPZ2H0PSIXM3QIIC8+CIAGICAGIDWVYNBTBMRPOKJQTU5TAGFWZT4K
ICAGICAGPGJWBW5KATPCUE10WRNRNZSBPZD0IQXNZB2NPYXRPB25FMTVYCHNRMF9KASIGYNBTBKVSZW1LBNQ9IKFZC29JAWF0AW9UXZE1CNB
ZAZAIPGOGICAGICAGIDKATP3YXLBW2LUDCB4PSI2MDAIHHK9IJJ1NTCIIIC8+CIAGICAGICAGPGRONDHEXBAW50IHG9IJJUYOCIGET0IM
JUSNSIGLZ4KICAGICAGPC9ICG1UZGK6QLBNTKVKZ2U+CIAGICAGICA8L2JWBW5KATPCUE10UGXHBMU+CIAGPC9ICG1UZGK6QLBNTKVKZ2U
+CJWVYNBTB3PKZWBPML0AW9UCZ4K"

```

    },
    "DETECTION_IDS": [
        "X-DEMO-ORG-DETECTION--58834C29-4CEB-42A1-A218-336103021000",
        "X-DEMO-ORG-DETECTION--458C02C9-3635-42E4-8873-6785E00517E7",
    ]

```

```
"X-DEMO-ORG-DETECTION--58834C29-4CEB-42A1-A218-336103021111",
"X-DEMO-ORG-DETECTION--58834C29-4CEB-42A1-A218-336103021222",
"X-DEMO-ORG-DETECTION--5899C5CC-CE20-44EE-806E-9F64EBA0B29F",
"X-DEMO-ORG-DETECTION--275BF485-736D-4AA5-B172-E34D28FAA58C",
"X-DEMO-ORG-DETECTION--F27CB358-D747-47BA-A6C4-E5B8DEBAB157",
"X-DEMO-ORG-DETECTION--40A941CC-42DF-4B2E-B607-6D74168084B9",
"X-DEMO-ORG-DETECTION--66AA9C25-8B56-4121-8630-DBE457393B27"
]
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-111111111111",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "DETECTS",
  "SOURCE_REF": "X-DEMO-ORG-DETECTION-GROUP--58834C29-4CEB-42A1-A218-321103021999",
  "TARGET_REF": "GROUPING--CB508D31-469C-41D0-AB3D-FB78ED60B61D"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--64726807-5082-43C3-B975-1484B60B963C",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "CONTAINS",
  "SOURCE_REF": "X-DEMO-ORG-DETECTION-GROUP--58834C29-4CEB-42A1-A218-321103021999",
  "TARGET_REF": "X-DEMO-ORG-DETECTION--66AA9C25-8B56-4121-8630-DBE457393B27"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--64726807-5082-43C3-B975-1484B60B963C",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "CONTAINS",
  "SOURCE_REF": "X-DEMO-ORG-DETECTION-GROUP--58834C29-4CEB-42A1-A218-321103021999",
  "TARGET_REF": "X-DEMO-ORG-DETECTION--40A941CC-42DF-4B2E-B607-6D74168084B9"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--64726807-5082-43C3-B975-1484B60B963C",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "CONTAINS",
  "SOURCE_REF": "X-DEMO-ORG-DETECTION-GROUP--58834C29-4CEB-42A1-A218-321103021999",
  "TARGET_REF": "X-DEMO-ORG-DETECTION--275BF485-736D-4AA5-B172-E34D28FAA58C"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--64726807-5082-43C3-B975-1484B60B963D",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "CONTAINS",
  "SOURCE_REF": "X-DEMO-ORG-DETECTION-GROUP--58834C29-4CEB-42A1-A218-321103021999",
  "TARGET_REF": "X-DEMO-ORG-DETECTION--F27CB358-D747-47BA-A6C4-E5B8DEBAB157"
},
{
  "TYPE": "RELATIONSHIP",
  "SPEC_VERSION": "2.1",
  "ID": "RELATIONSHIP--64726807-5082-43C3-B975-1484B60B963B",
  "CREATED": "2022-03-31T13:00:00.000Z",
  "MODIFIED": "2022-03-31T13:00:00.000Z",
  "RELATIONSHIP_TYPE": "CONTAINS",
  "SOURCE_REF": "X-DEMO-ORG-DETECTION-GROUP--58834C29-4CEB-42A1-A218-321103021999",
  "TARGET_REF": "X-DEMO-ORG-DETECTION--5899C5CC-CE20-44EE-806E-9F64EBA0B29F"
```

```

    },
    {
      "TYPE": "RELATIONSHIP",
      "SPEC_VERSION": "2.1",
      "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-11111111222",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "RELATIONSHIP_TYPE": "CONTAINS",
      "SOURCE_REF": "X-DEMO-ORG-DETECTION-GROUP--58834C29-4CEB-42A1-A218-321103021999",
      "TARGET_REF": "X-DEMO-ORG-DETECTION--58834C29-4CEB-42A1-A218-336103021000"
    },
    {
      "TYPE": "RELATIONSHIP",
      "SPEC_VERSION": "2.1",
      "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-11111111333",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "RELATIONSHIP_TYPE": "CONTAINS",
      "SOURCE_REF": "X-DEMO-ORG-DETECTION-GROUP--58834C29-4CEB-42A1-A218-321103021999",
      "TARGET_REF": "X-DEMO-ORG-DETECTION--458C02C9-3635-42E4-8873-6785E00517E7"
    },
    {
      "TYPE": "RELATIONSHIP",
      "SPEC_VERSION": "2.1",
      "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-11111111444",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "RELATIONSHIP_TYPE": "CONTAINS",
      "SOURCE_REF": "X-DEMO-ORG-DETECTION-GROUP--58834C29-4CEB-42A1-A218-321103021999",
      "TARGET_REF": "X-DEMO-ORG-DETECTION--58834C29-4CEB-42A1-A218-336103021111"
    },
    {
      "TYPE": "RELATIONSHIP",
      "SPEC_VERSION": "2.1",
      "ID": "RELATIONSHIP--37AC0C8D-F86D-4E56-AEE9-11111111555",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "RELATIONSHIP_TYPE": "CONTAINS",
      "SOURCE_REF": "X-DEMO-ORG-DETECTION-GROUP--58834C29-4CEB-42A1-A218-321103021999",
      "TARGET_REF": "X-DEMO-ORG-DETECTION--58834C29-4CEB-42A1-A218-336103021222"
    },
    {
      "TYPE": "EXTENSION-DEFINITION",
      "SPEC_VERSION": "2.1",
      "ID": "EXTENSION-DEFINITION--3B7505CE-2A18-496E-AA58-311DAC6C1473",
      "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "NAME": "NETWORK TRAFFIC EXTENSION DEFINITION",
      "SCHEMA": "TBD",
      "VERSION": "1.0.0",
      "EXTENSION_TYPES": [
        "PROPERTY-EXTENSION"
      ]
    },
    {
      "TYPE": "EXTENSION-DEFINITION",
      "SPEC_VERSION": "2.1",
      "ID": "EXTENSION-DEFINITION--2CF8C8C2-69F5-40F7-AA34-EFCEF2B912B1",
      "CREATED_BY_REF": "IDENTITY--B085A68A-BF48-4316-9667-37AF78CBA894",
      "CREATED": "2022-03-31T13:00:00.000Z",
      "MODIFIED": "2022-03-31T13:00:00.000Z",
      "NAME": "WINDOWS REGISTRY KEY EXTENSION DEFINITION",
      "SCHEMA": "TBD",
      "VERSION": "1.0.0",
      "EXTENSION_TYPES": [
        "PROPERTY-EXTENSION"
      ]
    }
  ]

```



}
]
}