

|  |  |
| --- | --- |
|  | BÁO CÁO RÀ QUÉT MÃ ĐỘC |
|  |  |
| 14/12/2020 | LẠNG SƠN |
|  |  |

**BÁO CÁO RÀ QUÉT MÃ ĐỘC**

MÁY CHỦ LẠNG SƠN

1. VĂN PHÒNG UBND TỈNH
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_VP UBND TINH | 0 | 0 | 0 | 0 |

1. VĂN PHÒNG HĐND TỈNH
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_VP HDND TINH | 2 | 3 | 0 | 3 |
| 1.1 | *Nhóm*: Phục vụ | 1 | 2 | 0 | 2 |
| 1.2 | *Nhóm*: Phòng Ban Trực Thuộc | 1 | 1 | 0 | 1 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | HNDIEP | D05099869E98 | 10.116.10.160 | [LS] LS\_VP HDND TINH | Phục vụ | 2 |
| 2 | DESKTOP-PV62VK1 | 2CF05D2AFFE4 | 10.116.11.77 | [LS] LS\_VP HDND TINH | Phòng Ban Trực Thuộc | 1 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 1 |
| 2 | [trojan.win32.hjclient.lnk.s!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.hjclient.lnk.s!o) | 5 | 2 |

1. SỞ THÔNG TIN VÀ TRUYỀN THÔNG
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_SO THONG TIN VA TRUYEN THONG | 0 | 0 | 0 | 0 |

1. SỞ VĂN HÓA THỂ THAO VÀ DU LỊCH
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_SO VAN HOA THE THAO VA DU LICH | 4 | 8 | 2 | 6 |
| 1.1 | *Nhóm*: Văn Phòng Sở | 1 | 2 | 0 | 2 |
| 1.2 | *Nhóm*: Phòng Quản Lý Văn Hoá và Gia đình | 2 | 4 | 2 | 2 |
| 1.3 | *Nhóm*: Thanh Tra | 1 | 2 | 0 | 2 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | ADMIN-1219YTC | 5404A6C06D02 | 10.0.0.159 | [LS] LS\_SO VAN HOA THE THAO VA DU LICH | Phòng Quản Lý Văn Hoá và Gia đình | 2 |
| 2 | PF995MS9ZAD4UWZ | B8975A5C0F41 | 192.168.1.101 | [LS] LS\_SO VAN HOA THE THAO VA DU LICH | Văn Phòng Sở | 2 |
| 3 | VANANHVH | FCAA143C2C2F | 10.0.0.198 | [LS] LS\_SO VAN HOA THE THAO VA DU LICH | Phòng Quản Lý Văn Hoá và Gia đình | 2 |
| 4 | ANJ-20181210HWF | 408D5C3B5A48 | 10.0.0.31 | [LS] LS\_SO VAN HOA THE THAO VA DU LICH | Thanh Tra | 2 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.wminer4.s!m](https://cloud.cmdd.vn/detail/virus/trojan.win32.wminer4.s!m) | 5 | 6 |
| 2 | [hacktool.win32.kmsauto.i!o](https://cloud.cmdd.vn/detail/virus/hacktool.win32.kmsauto.i!o) | 1 | 2 |

1. SỞ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_SO NONG NGHIEP VA PTNT | 8 | 830 | 17 | 813 |
| 1.1 | *Nhóm*: Chi cục Phát triển nông thôn | 1 | 2 | 0 | 2 |
| 1.2 | *Nhóm*: Chi cục Chăn nuôi và Thú y | 1 | 1 | 0 | 1 |
| 1.3 | *Nhóm*: Trung tâm Nước sạch và VS MT NT | 1 | 4 | 0 | 4 |
| 1.4 | *Nhóm*: Phòng Tổ chức cán bộ | 1 | 1 | 0 | 1 |
| 1.5 | *Nhóm*: Chi cục Kiểm lâm | 2 | 782 | 8 | 774 |
| 1.6 | *Nhóm*: Thanh tra Sở | 1 | 30 | 0 | 30 |
| 1.7 | *Nhóm*: Phòng Kế hoạch Tài chính | 1 | 10 | 9 | 1 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | DESKTOP-K2KA8I5 | D45D648371B8 | 192.168.1.37 | [LS] LS\_SO NONG NGHIEP VA PTNT | Phòng Tổ chức cán bộ | 1 |
| 2 | YRCJOQ4W9JHUDJC | 00E04C6488B6 | 192.168.1.215 | [LS] LS\_SO NONG NGHIEP VA PTNT | Thanh tra Sở | 30 |
| 3 | ABTT-20190318YM | 8416F90630EE | 192.168.1.114 | [LS] LS\_SO NONG NGHIEP VA PTNT | Phòng Kế hoạch Tài chính | 10 |
| 4 | ADMIN-D6E4E4DEE | 0022685DDA11 | 192.168.0.111 | [LS] LS\_SO NONG NGHIEP VA PTNT | Chi cục Kiểm lâm | 780 |
| 5 | GIGABYTE-PC | 300ED5195BC4 | 192.168.1.12 | [LS] LS\_SO NONG NGHIEP VA PTNT | Trung tâm Nước sạch và VS MT NT | 4 |
| 6 | WINDOWS-PC | 90FBA627B725 | 192.168.10.112 | [LS] LS\_SO NONG NGHIEP VA PTNT | Chi cục Chăn nuôi và Thú y | 1 |
| 7 | DELL-PC | F8BC12A23F2D | 192.168.1.19 | [LS] LS\_SO NONG NGHIEP VA PTNT | Chi cục Kiểm lâm | 2 |
| 8 | ABC123 | A08CFDEA9455 | 192.168.1.101 | [LS] LS\_SO NONG NGHIEP VA PTNT | Chi cục Phát triển nông thôn | 2 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 8 |
| 2 | [trojan.win32.fakeusb!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.fakeusb!o) | 5 | 2 |
| 3 | [virus.win32.ramit.1!o](https://cloud.cmdd.vn/detail/virus/virus.win32.ramit.1!o) | 3 | 770 |
| 4 | [worm.win32.autorun!o](https://cloud.cmdd.vn/detail/virus/worm.win32.autorun!o) | 2 | 6 |
| 5 | [Trojan.MSIL.Disfa!O](https://cloud.cmdd.vn/detail/virus/Trojan.MSIL.Disfa!O) | 5 | 10 |
| 6 | [trojan.html.script03.p!o](https://cloud.cmdd.vn/detail/virus/trojan.html.script03.p!o) | 5 | 1 |
| 7 | [trojan-gamethief.win32.magani!o](https://cloud.cmdd.vn/detail/virus/trojan-gamethief.win32.magani!o) | 5 | 30 |
| 8 | [trojan.html.script00.p!o](https://cloud.cmdd.vn/detail/virus/trojan.html.script00.p!o) | 5 | 3 |

1. SỞ Y TẾ
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_SO Y TE | 3 | 85 | 0 | 85 |
| 1.1 | *Nhóm*: Phòng Kế hoạch TC | 1 | 76 | 0 | 76 |
| 1.2 | *Nhóm*: Lãnh Đạo | 1 | 1 | 0 | 1 |
| 1.3 | *Nhóm*: Phòng Thanh tra | 1 | 8 | 0 | 8 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | ADMIN-PC | 408D5CFD7FA0 | 192.168.1.101 | [LS] LS\_SO Y TE | Lãnh Đạo | 1 |
| 2 | LY-KT | 484D7EB02992 | 10.116.29.26 | [LS] LS\_SO Y TE | Phòng Kế hoạch TC | 76 |
| 3 | MAYTINHNHATSON | 1C1B0D8E2EE5 | 10.116.29.13 | [LS] LS\_SO Y TE | Phòng Thanh tra | 8 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.patched.qw!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.patched.qw!o) | 5 | 76 |
| 2 | [hacktool.win32.wincred.b!o](https://cloud.cmdd.vn/detail/virus/hacktool.win32.wincred.b!o) | 1 | 8 |
| 3 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 1 |

1. SỞ GIÁO DỤC VÀ ĐÀO TẠO
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_SO GIAO DUC VA DAO TAO | 2 | 15 | 14 | 1 |
| 1.1 | *Nhóm*: Văn phòng Sở | 2 | 15 | 14 | 1 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | DESKTOP-7TIKRLN | 1C1B0DD2ADC1 | 10.116.27.228 | [LS] LS\_SO GIAO DUC VA DAO TAO | Văn phòng Sở | 14 |
| 2 | ANH\_TUAN | 00090FFE0001 | 10.116.26.195 | [LS] LS\_SO GIAO DUC VA DAO TAO | Văn phòng Sở | 1 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [adware.win32.popupguide!o](https://cloud.cmdd.vn/detail/virus/adware.win32.popupguide!o) | 2 | 14 |
| 2 | [heur.win32.autoruninf.p](https://cloud.cmdd.vn/detail/virus/heur.win32.autoruninf.p) | 1 | 1 |

1. THANH TRA TỈNH
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_THANH TRA TINH | 0 | 0 | 0 | 0 |

1. SỞ TƯ PHÁP
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_So Tu phap | 1 | 32 | 0 | 32 |
| 1.1 | *Nhóm*: Thanh tra | 1 | 32 | 0 | 32 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | DESKTOP-RN61OOD | 8CEC4BBF59A5 | 10.116.28.57 | [LS] LS\_So Tu phap | Thanh tra | 32 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 32 |

1. SỞ TÀI NGUYÊN MÔI TRƯỜNG
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_So Tai nguyen va Moi truong | 1 | 3 | 0 | 3 |
| 1.1 | *Nhóm*: Phòng Quản lý đất đai | 1 | 3 | 0 | 3 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | DESKTOP-SS87CD4 | 8C8590807CE3 | 192.168.1.110 | [LS] LS\_So Tai nguyen va Moi truong | Phòng Quản lý đất đai | 3 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan-ransom.win32.blocker!o](https://cloud.cmdd.vn/detail/virus/trojan-ransom.win32.blocker!o) | 5 | 3 |

1. SỞ TÀI CHÍNH
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_So Tai Chinh | 0 | 0 | 0 | 0 |

1. SỞ NỘI VỤ
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_So Noi Vu | 1 | 1 | 0 | 1 |
| 1.1 | *Nhóm*: Văn phòng sở | 1 | 1 | 0 | 1 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | SONOIVU-TONGIAO | D02788B40A01 | 10.116.50.30 | [LS] LS\_So Noi Vu | Văn phòng sở | 1 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 1 |

1. SỞ NGOẠI VỤ
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_So Ngoai Vu | 0 | 0 | 0 | 0 |

1. SỞ LAO ĐỘNG TB XH
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_So LD TB va XH | 0 | 0 | 0 | 0 |

1. SỞ KẾ HOẠCH VÀ ĐẦU TƯ
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_So Ke hoach va Dau tu | 0 | 0 | 0 | 0 |

1. SỞ CÔNG THƯƠNG
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_So Cong thuong | 1 | 48 | 44 | 4 |
| 1.1 | *Nhóm*: Phòng Quản lý Thương mại | 1 | 48 | 44 | 4 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | ADMINISTRATOR | 002268461024 | 192.168.0.107 | [LS] LS\_So Cong thuong | Phòng Quản lý Thương mại | 48 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.fakeapp!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.fakeapp!o) | 5 | 48 |

1. SỞ XÂY DỰNG
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_SO XAY DUNG | 2 | 4 | 0 | 4 |
| 1.1 | *Nhóm*: Văn phòng Sở | 1 | 2 | 0 | 2 |
| 1.2 | *Nhóm*: Phòng Quy hoạch - kiến trúc và phát triển đô thị | 1 | 2 | 0 | 2 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | HD-PC | FCAA1408BF81 | 10.116.40.123 | [LS] LS\_SO XAY DUNG | Phòng Quy hoạch - kiến trúc và phát triển đô thị | 2 |
| 2 | CHUHUYENTRANG | D050994B52E2 | 10.116.40.118 | [LS] LS\_SO XAY DUNG | Văn phòng Sở | 2 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.wminer4.s!m](https://cloud.cmdd.vn/detail/virus/trojan.win32.wminer4.s!m) | 5 | 4 |

1. SỞ GIAO THÔNG VẬN TẢI
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_SO GIAO THONG VAN TAI | 2 | 12 | 0 | 12 |
| 1.1 | *Nhóm*: Văn phòng Sở | 1 | 10 | 0 | 10 |
| 1.2 | *Nhóm*: Quản lý kết cấu hạ tầng và An toàn giao thông | 1 | 2 | 0 | 2 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | KCHT-DVTAM | 04D4C424D1C6 | 10.116.36.241 | [LS] LS\_SO GIAO THONG VAN TAI | Quản lý kết cấu hạ tầng và An toàn giao thông | 2 |
| 2 | DTNHOA-VP | F4B520064DB3 | 10.116.36.170 | [LS] LS\_SO GIAO THONG VAN TAI | Văn phòng Sở | 10 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [ransom.win32.wannacry.s!m](https://cloud.cmdd.vn/detail/virus/ransom.win32.wannacry.s!m) | 2 | 10 |
| 2 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 2 |

1. THÀNH PHỐ
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_THANH PHO | 13 | 91 | 50 | 41 |
| 1.1 | *Nhóm*: UBND phường Vĩnh Trại | 1 | 2 | 0 | 2 |
| 1.2 | *Nhóm*: Phòng Tư pháp TP | 1 | 4 | 0 | 4 |
| 1.3 | *Nhóm*: UBND phường HVT | 1 | 3 | 0 | 3 |
| 1.4 | *Nhóm*: UBND phường Chi Lăng | 4 | 9 | 4 | 5 |
| 1.5 | *Nhóm*: UBND phường Đông Kinh | 1 | 48 | 46 | 2 |
| 1.6 | *Nhóm*: Phòng Nội vụ TP | 1 | 2 | 0 | 2 |
| 1.7 | *Nhóm*: Phòng VH và TT TP | 2 | 4 | 0 | 4 |
| 1.8 | *Nhóm*: UBND xã Quảng Lạc | 1 | 12 | 0 | 12 |
| 1.9 | *Nhóm*: Phòng TNMT TPLS | 1 | 7 | 0 | 7 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | PHONGVANHOA-PC | AC220BC80228 | 192.168.1.8 | [LS] LS\_THANH PHO | Phòng VH và TT TP | 2 |
| 2 | TINHTULS | 1C1B0DD27577 | 192.168.1.11 | [LS] LS\_THANH PHO | UBND phường Đông Kinh | 48 |
| 3 | PC2019051310NRF | 000206081138 | 10.116.128.12 | [LS] LS\_THANH PHO | UBND phường Chi Lăng | 1 |
| 4 | DESKTOP-ABHG61A | F4B5200762E6 | 192.168.0.114 | [LS] LS\_THANH PHO | UBND xã Quảng Lạc | 12 |
| 5 | DESKTOP-NDP5LJC | B42E99539774 | 10.0.0.71 | [LS] LS\_THANH PHO | Phòng Tư pháp TP | 4 |
| 6 | 4ECY0YKEPD7RKQI | 00E04CFC1D3C | 10.116.128.35 | [LS] LS\_THANH PHO | UBND phường Chi Lăng | 2 |
| 7 | 0L9MQL39E55NUWV | E0D55E05FB56 | 10.116.128.28 | [LS] LS\_THANH PHO | UBND phường Chi Lăng | 2 |
| 8 | DESKTOP-HUC7H72 | 7440BB00178B | 192.168.1.57 | [LS] LS\_THANH PHO | Phòng TNMT TPLS | 7 |
| 9 | CTT0126ZMR | 2025640A7DC4 | 192.168.1.9 | [LS] LS\_THANH PHO | Phòng VH và TT TP | 2 |
| 10 | TNHTU-PC | B8975AFE40D5 | 192.168.1.30 | [LS] LS\_THANH PHO | UBND phường HVT | 3 |
| 11 | C6S0WAR8TMC8E8L | FCAA1408802B | 10.0.0.5 | [LS] LS\_THANH PHO | Phòng Nội vụ TP | 2 |
| 12 | PC2019050617KFB | 8416F91C55DE | 192.168.0.124 | [LS] LS\_THANH PHO | UBND phường Chi Lăng | 4 |
| 13 | PC-PC | FCAA14FE47B1 | 192.168.1.29 | [LS] LS\_THANH PHO | UBND phường Vĩnh Trại | 2 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.wminer4.s!m](https://cloud.cmdd.vn/detail/virus/trojan.win32.wminer4.s!m) | 5 | 12 |
| 2 | [backdoor.win32.dragonbot!o](https://cloud.cmdd.vn/detail/virus/backdoor.win32.dragonbot!o) | 5 | 1 |
| 3 | [adware.win32!o](https://cloud.cmdd.vn/detail/virus/adware.win32!o) | 2 | 1 |
| 4 | [virus.win32.virut.1!o](https://cloud.cmdd.vn/detail/virus/virus.win32.virut.1!o) | 3 | 1 |
| 5 | [risktool.win32.bitcoinminer!o](https://cloud.cmdd.vn/detail/virus/risktool.win32.bitcoinminer!o) | 2 | 4 |
| 6 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 60 |
| 7 | [trojan.win32.startpage!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.startpage!o) | 5 | 1 |
| 8 | [trojan.win32.fakeapp!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.fakeapp!o) | 5 | 3 |
| 9 | [adware.win32.navexcel!o](https://cloud.cmdd.vn/detail/virus/adware.win32.navexcel!o) | 2 | 1 |
| 10 | [trojan-ransom.win32.blocker!o](https://cloud.cmdd.vn/detail/virus/trojan-ransom.win32.blocker!o) | 5 | 7 |

1. HUYỆN VĂN LÃNG
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_HUYEN VAN LANG | 23 | 13258 | 11750 | 1508 |
| 1.1 | *Nhóm*: Xã Thụy Hùng | 2 | 26 | 25 | 1 |
| 1.2 | *Nhóm*: Văn phòng huyện | 4 | 29 | 0 | 29 |
| 1.3 | *Nhóm*: Xã Hoàng Việt | 5 | 11 | 7 | 4 |
| 1.4 | *Nhóm*: Xã Thanh Long | 1 | 21 | 0 | 21 |
| 1.5 | *Nhóm*: Xã Hoàng Văn Thụ | 2 | 5 | 0 | 5 |
| 1.6 | *Nhóm*: Phòng Văn hoá và Thông tin | 1 | 65 | 0 | 65 |
| 1.7 | *Nhóm*: Xã Gia Miễn | 1 | 11 | 0 | 11 |
| 1.8 | *Nhóm*: Phòng Tư pháp | 1 | 13058 | 11717 | 1341 |
| 1.9 | *Nhóm*: Xã Bắc Việt | 1 | 2 | 0 | 2 |
| 1.10 | *Nhóm*: Trung tâm GDNN GDTX | 1 | 1 | 0 | 1 |
| 1.11 | *Nhóm*: Xã Hội Hoan | 2 | 4 | 0 | 4 |
| 1.12 | *Nhóm*: Xã Bắc La | 2 | 25 | 1 | 24 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | ADMINISTRATOR | 74D4356D9287 | 192.168.1.7 | [LS] LS\_HUYEN VAN LANG | Xã Bắc La | 24 |
| 2 | ADMIN | 408D5CA15B8A | 10.116.68.33 | [LS] LS\_HUYEN VAN LANG | Văn phòng huyện | 17 |
| 3 | NZAF6VMH5V54EOV | 7CA7B0CA1664 | 192.168.1.111 | [LS] LS\_HUYEN VAN LANG | Xã Thanh Long | 21 |
| 4 | QFWHCJ6GD9Y5M6J | 78843C3745CF | 10.116.68.24 | [LS] LS\_HUYEN VAN LANG | Văn phòng huyện | 6 |
| 5 | DYMOESUEXPZUKJ0 | 40E230B24EF2 | 192.168.1.6 | [LS] LS\_HUYEN VAN LANG | Xã Thụy Hùng | 8 |
| 6 | 2XINH-20200224X | 04D9F55DCD2A | 192.168.1.113 | [LS] LS\_HUYEN VAN LANG | Xã Gia Miễn | 11 |
| 7 | PC2019032511TYP | AC220BCBA0DB | 192.168.1.102 | [LS] LS\_HUYEN VAN LANG | Phòng Tư pháp | 13058 |
| 8 | ADMIN | 303A64BF31E6 | 10.116.165.58 | [LS] LS\_HUYEN VAN LANG | Xã Hội Hoan | 1 |
| 9 | 2XINH-20191223X | A85E45112BAA | 192.168.1.254 | [LS] LS\_HUYEN VAN LANG | Xã Hoàng Văn Thụ | 4 |
| 10 | 9GMEKI3GR0MDRD6 | FCAA14174A68 | 10.116.68.11 | [LS] LS\_HUYEN VAN LANG | Văn phòng huyện | 1 |
| 11 | 2XINH-20200716N | 00E04B3604E3 | 192.168.0.100 | [LS] LS\_HUYEN VAN LANG | Xã Bắc La | 1 |
| 12 | PC1 | DC85DE93B65D | 192.168.1.32 | [LS] LS\_HUYEN VAN LANG | Phòng Văn hoá và Thông tin | 65 |
| 13 | 2XINH-20200428B | 1C1B0DB66025 | 192.168.1.6 | [LS] LS\_HUYEN VAN LANG | Xã Hoàng Văn Thụ | 1 |
| 14 | 2XINH-20200318T | A85E45B26CA3 | 192.168.0.102 | [LS] LS\_HUYEN VAN LANG | Xã Hoàng Việt | 4 |
| 15 | 2XINH-20181223I | 94DE80FCFF46 | 192.168.1.21 | [LS] LS\_HUYEN VAN LANG | Xã Hoàng Việt | 2 |
| 16 | DESKTOP-H35MQHD | A85E451130D4 | 192.168.1.16 | [LS] LS\_HUYEN VAN LANG | Xã Hoàng Việt | 2 |
| 17 | 2XINH-20190302B | B8975AEA5830 | 10.116.68.28 | [LS] LS\_HUYEN VAN LANG | Văn phòng huyện | 5 |
| 18 | W4SB512UKKNAWC8 | 74D435C750D2 | 192.168.1.214 | [LS] LS\_HUYEN VAN LANG | Xã Hoàng Việt | 1 |
| 19 | 6ZBQR2168TM0JAB | 74EE2AF09C98 | 192.168.1.20 | [LS] LS\_HUYEN VAN LANG | Xã Hoàng Việt | 2 |
| 20 | DELL0-PC | 44032CD7EBE1 | 192.168.1.7 | [LS] LS\_HUYEN VAN LANG | Xã Hội Hoan | 3 |
| 21 | 2XINH-20190318T | 40167EA82515 | 192.168.0.152 | [LS] LS\_HUYEN VAN LANG | Trung tâm GDNN GDTX | 1 |
| 22 | Q2Y2STRUD5SVWX0 | 146B9C02C082 | 192.168.1.114 | [LS] LS\_HUYEN VAN LANG | Xã Thụy Hùng | 18 |
| 23 | MAY19 | 00E04C14653F | 192.168.1.8 | [LS] LS\_HUYEN VAN LANG | Xã Bắc Việt | 2 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.gamaru.s!m](https://cloud.cmdd.vn/detail/virus/trojan.win32.gamaru.s!m) | 5 | 18 |
| 2 | [virus.win32.virut.1!o](https://cloud.cmdd.vn/detail/virus/virus.win32.virut.1!o) | 3 | 1 |
| 3 | [trojan.win32.csyr!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.csyr!o) | 5 | 3 |
| 4 | [trojan-spy.win32.keylogger!o](https://cloud.cmdd.vn/detail/virus/trojan-spy.win32.keylogger!o) | 5 | 1 |
| 5 | [trojan-downloader.win32.trik!o](https://cloud.cmdd.vn/detail/virus/trojan-downloader.win32.trik!o) | 5 | 1 |
| 6 | [heur.win32.autoruninf.p](https://cloud.cmdd.vn/detail/virus/heur.win32.autoruninf.p) | 1 | 6 |
| 7 | [worm.win32.bundpil!o](https://cloud.cmdd.vn/detail/virus/worm.win32.bundpil!o) | 2 | 1 |
| 8 | [trojan.win32.generiz.s!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.generiz.s!o) | 5 | 60 |
| 9 | [trojan.win32.agent!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.agent!o) | 5 | 1 |
| 10 | [trojan.win32.fakeapp!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.fakeapp!o) | 5 | 13082 |
| 11 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 23 |
| 12 | [virus.win32.hvqb.s!o](https://cloud.cmdd.vn/detail/virus/virus.win32.hvqb.s!o) | 3 | 27 |
| 13 | [backdoor.win32.androm!o](https://cloud.cmdd.vn/detail/virus/backdoor.win32.androm!o) | 5 | 6 |
| 14 | [adware.win32.agent!o](https://cloud.cmdd.vn/detail/virus/adware.win32.agent!o) | 2 | 2 |
| 15 | [trojan.win32.patched.qw!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.patched.qw!o) | 5 | 10 |
| 16 | [trojan-dropper.win32!o](https://cloud.cmdd.vn/detail/virus/trojan-dropper.win32!o) | 5 | 1 |
| 17 | [Trojan-Downloader.Win32.Trik!O](https://cloud.cmdd.vn/detail/virus/Trojan-Downloader.Win32.Trik!O) | 5 | 15 |

1. HUYỆN HỮU LŨNG
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_HUYEN HUU LUNG | 0 | 0 | 0 | 0 |

1. HUYỆN ĐÌNH LẬP
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_HUYEN DINH LAP | 6 | 411 | 395 | 16 |
| 1.1 | *Nhóm*: UBND xã Đình Lập | 2 | 215 | 212 | 3 |
| 1.2 | *Nhóm*: UBND xã Lâm Ca | 4 | 196 | 183 | 13 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | DELL-PC | F8B156B1B292 | 192.168.1.13 | [LS] LS\_HUYEN DINH LAP | UBND xã Lâm Ca | 191 |
| 2 | PC2017040311UZF | 74C63B0877E1 | 192.168.1.7 | [LS] LS\_HUYEN DINH LAP | UBND xã Lâm Ca | 2 |
| 3 | ADMINISTRATOR | 00E04C997296 | 192.168.1.4 | [LS] LS\_HUYEN DINH LAP | UBND xã Lâm Ca | 1 |
| 4 | ADMIN | 742F6899D207 | 192.168.1.2 | [LS] LS\_HUYEN DINH LAP | UBND xã Đình Lập | 30 |
| 5 | ADMIN | 00E04C443076 | 192.168.1.14 | [LS] LS\_HUYEN DINH LAP | UBND xã Đình Lập | 185 |
| 6 | ADMIN | 00E04C709E0A | 192.168.1.4 | [LS] LS\_HUYEN DINH LAP | UBND xã Lâm Ca | 2 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.patched.qw!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.patched.qw!o) | 5 | 5 |
| 2 | [trojan.win32.shelma.qlc!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shelma.qlc!o) | 5 | 9 |
| 3 | [trojan.win32.agentb.isqc!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.agentb.isqc!o) | 5 | 5 |
| 4 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 370 |
| 5 | [backdoor.win32.ruskill!o](https://cloud.cmdd.vn/detail/virus/backdoor.win32.ruskill!o) | 5 | 19 |
| 6 | [trojan.win32.wminer4.s!m](https://cloud.cmdd.vn/detail/virus/trojan.win32.wminer4.s!m) | 5 | 3 |

1. HUYỆN CHI LĂNG
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_HUYEN CHI LANG | 3 | 30 | 4 | 26 |
| 1.1 | *Nhóm*: UBND xã Vạn Linh | 1 | 3 | 0 | 3 |
| 1.2 | *Nhóm*: Thanh tra huyện | 1 | 1 | 0 | 1 |
| 1.3 | *Nhóm*: Phòng Tài chính Kế hoạch | 1 | 26 | 4 | 22 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | BAC-PC | 7CE9D39AE379 | 192.168.0.103 | [LS] LS\_HUYEN CHI LANG | UBND xã Vạn Linh | 3 |
| 2 | PC2018022208HTE | B8975AB39371 | 192.168.1.34 | [LS] LS\_HUYEN CHI LANG | Thanh tra huyện | 1 |
| 3 | HUONG | 4401BB929A98 | 192.168.3.107 | [LS] LS\_HUYEN CHI LANG | Phòng Tài chính Kế hoạch | 26 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [virus.win32.hvqb.s!o](https://cloud.cmdd.vn/detail/virus/virus.win32.hvqb.s!o) | 3 | 26 |
| 2 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 1 |
| 3 | [trojan-ransom.win32.blocker!o](https://cloud.cmdd.vn/detail/virus/trojan-ransom.win32.blocker!o) | 5 | 3 |

1. HUYỆN CAO LỘC
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_HUYEN CAO LOC | 6 | 241 | 219 | 22 |
| 1.1 | *Nhóm*: Lãnh đạo UBND | 2 | 226 | 219 | 7 |
| 1.2 | *Nhóm*: UBND Xã Gia Cát | 1 | 5 | 0 | 5 |
| 1.3 | *Nhóm*: UBND Xã Tân Thành | 1 | 5 | 0 | 5 |
| 1.4 | *Nhóm*: UBND Xã Hải Yến | 1 | 1 | 0 | 1 |
| 1.5 | *Nhóm*: UBND Xã Lộc Yên | 1 | 4 | 0 | 4 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | CV\_THANH | 3C7C3FD6E63E | 192.168.1.190 | [LS] LS\_HUYEN CAO LOC | Lãnh đạo UBND | 63 |
| 2 | ADMINISTRATOR | F4B52000BD90 | 192.168.1.11 | [LS] LS\_HUYEN CAO LOC | UBND Xã Lộc Yên | 4 |
| 3 | TN-PC | BC8556524DCD | 192.168.1.129 | [LS] LS\_HUYEN CAO LOC | UBND Xã Tân Thành | 5 |
| 4 | HD-PC | B8763F26B83F | 192.168.1.5 | [LS] LS\_HUYEN CAO LOC | UBND Xã Gia Cát | 5 |
| 5 | LEQUANG-PC | 7085C20193EA | 192.168.0.102 | [LS] LS\_HUYEN CAO LOC | UBND Xã Hải Yến | 1 |
| 6 | ADMIN | B8975AE1B923 | 192.168.1.30 | [LS] LS\_HUYEN CAO LOC | Lãnh đạo UBND | 163 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 23 |
| 2 | [virus.win32.ramit.1!o](https://cloud.cmdd.vn/detail/virus/virus.win32.ramit.1!o) | 3 | 60 |
| 3 | [trojan.win32.fakeapp!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.fakeapp!o) | 5 | 36 |
| 4 | [hacktool.win32.kmsauto.er!o](https://cloud.cmdd.vn/detail/virus/hacktool.win32.kmsauto.er!o) | 1 | 1 |
| 5 | [trojan.win32.gamaru.s!m](https://cloud.cmdd.vn/detail/virus/trojan.win32.gamaru.s!m) | 5 | 1 |
| 6 | [trojan.win32.agent.ifdx!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.agent.ifdx!o) | 5 | 62 |
| 7 | [trojan.win32!o](https://cloud.cmdd.vn/detail/virus/trojan.win32!o) | 5 | 9 |
| 8 | [virus.win32.virut.1!o](https://cloud.cmdd.vn/detail/virus/virus.win32.virut.1!o) | 3 | 32 |
| 9 | [heur.win32.autoruninf.p](https://cloud.cmdd.vn/detail/virus/heur.win32.autoruninf.p) | 1 | 4 |
| 10 | [trojan.win32.patched.qw!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.patched.qw!o) | 5 | 8 |
| 11 | [trojan.win32.agent!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.agent!o) | 5 | 1 |
| 12 | [trojan-ransom.win32.blocker!o](https://cloud.cmdd.vn/detail/virus/trojan-ransom.win32.blocker!o) | 5 | 3 |
| 13 | [adware.win32.topmoxie!o](https://cloud.cmdd.vn/detail/virus/adware.win32.topmoxie!o) | 2 | 1 |

1. HUYỆN BÌNH GIA
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_HUYEN BINH GIA | 12 | 92 | 45 | 47 |
| 1.1 | *Nhóm*: Phòng Lao động, Thương binh và Xã hội - Dân tộc | 1 | 1 | 0 | 1 |
| 1.2 | *Nhóm*: UBND thị trấn Bình Gia | 2 | 12 | 10 | 2 |
| 1.3 | *Nhóm*: UBND xã Tân Văn | 2 | 21 | 1 | 20 |
| 1.4 | *Nhóm*: UBND xã Thiện Long | 1 | 2 | 0 | 2 |
| 1.5 | *Nhóm*: Văn Phòng HĐND và UBND | 2 | 36 | 34 | 2 |
| 1.6 | *Nhóm*: UBND xã Yên Lỗ | 1 | 9 | 0 | 9 |
| 1.7 | *Nhóm*: Phòng Kinh Tế Hạ Tầng | 1 | 8 | 0 | 8 |
| 1.8 | *Nhóm*: UBND xã Vĩnh Yên | 2 | 3 | 0 | 3 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | DESKTOP-PH9GPFV | B42E9973F9E1 | 192.168.1.5 | [LS] LS\_HUYEN BINH GIA | Phòng Lao động, Thương binh và Xã hội - Dân tộc | 1 |
| 2 | VANTHU-PC | 448A5B267768 | 192.168.1.137 | [LS] LS\_HUYEN BINH GIA | Văn Phòng HĐND và UBND | 34 |
| 3 | DESKTOP-7A873VH | B42E9947CEBF | 192.168.1.9 | [LS] LS\_HUYEN BINH GIA | UBND thị trấn Bình Gia | 2 |
| 4 | COMPUTER | 00E05D360421 | 192.168.1.73 | [LS] LS\_HUYEN BINH GIA | UBND xã Thiện Long | 2 |
| 5 | DUVINHYEN-PC | A41731E5C947 | 192.168.0.104 | [LS] LS\_HUYEN BINH GIA | UBND xã Vĩnh Yên | 1 |
| 6 | ASUS-PC | 28E347D1DF37 | 192.168.1.18 | [LS] LS\_HUYEN BINH GIA | UBND xã Vĩnh Yên | 2 |
| 7 | LENOVO-PC | 74DE2B58955F | 192.168.3.109 | [LS] LS\_HUYEN BINH GIA | UBND xã Yên Lỗ | 9 |
| 8 | 04KVWSU2RZ1WSGQ | 18D6C71FB69D | 192.168.0.107 | [LS] LS\_HUYEN BINH GIA | Phòng Kinh Tế Hạ Tầng | 8 |
| 9 | HP-PC | 0C96E6E17339 | 192.168.1.103 | [LS] LS\_HUYEN BINH GIA | UBND xã Tân Văn | 1 |
| 10 | TPTH-PC | 408D5CD56E54 | 192.168.16.108 | [LS] LS\_HUYEN BINH GIA | UBND thị trấn Bình Gia | 10 |
| 11 | ACER-PC | C0F8DA023882 | 192.168.1.110 | [LS] LS\_HUYEN BINH GIA | UBND xã Tân Văn | 20 |
| 12 | DESKTOP-43ADFP9 | B42E99C7DB1E | 192.168.1.140 | [LS] LS\_HUYEN BINH GIA | Văn Phòng HĐND và UBND | 2 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.wminer4.s!m](https://cloud.cmdd.vn/detail/virus/trojan.win32.wminer4.s!m) | 5 | 2 |
| 2 | [trojan.win32.gamaru.s!m](https://cloud.cmdd.vn/detail/virus/trojan.win32.gamaru.s!m) | 5 | 20 |
| 3 | [trojan-dropper.win32!o](https://cloud.cmdd.vn/detail/virus/trojan-dropper.win32!o) | 5 | 1 |
| 4 | [virus.win32.virut.1!o](https://cloud.cmdd.vn/detail/virus/virus.win32.virut.1!o) | 3 | 1 |
| 5 | [trojan.win32.patched.qw!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.patched.qw!o) | 5 | 2 |
| 6 | [hacktool.win32.kmsauto.i!o](https://cloud.cmdd.vn/detail/virus/hacktool.win32.kmsauto.i!o) | 1 | 2 |
| 7 | [trojan.win32.fakeapp!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.fakeapp!o) | 5 | 42 |
| 8 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 11 |
| 9 | [heur.win32.autoruninf.p](https://cloud.cmdd.vn/detail/virus/heur.win32.autoruninf.p) | 1 | 3 |
| 10 | [hoax.win32.deceptpcclean.dcp!o](https://cloud.cmdd.vn/detail/virus/hoax.win32.deceptpcclean.dcp!o) | 2 | 8 |

1. HUYỆN VĂN QUAN
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_HUYEN VAN QUAN | 11 | 266 | 58 | 208 |
| 1.1 | *Nhóm*: UBND Xã Đồng Giáp | 2 | 137 | 0 | 137 |
| 1.2 | *Nhóm*: UBND Xã Hoà Bình | 1 | 18 | 0 | 18 |
| 1.3 | *Nhóm*: UBND Xã Khánh Khê | 1 | 1 | 0 | 1 |
| 1.4 | *Nhóm*: UBND Xã Tú Xuyên | 1 | 13 | 0 | 13 |
| 1.5 | *Nhóm*: UBND Xã An Sơn | 2 | 55 | 54 | 1 |
| 1.6 | *Nhóm*: Trung tâm Văn hoá Thể thao và Truyền thông | 1 | 1 | 0 | 1 |
| 1.7 | *Nhóm*: UBND Xã Trấn Ninh | 2 | 5 | 4 | 1 |
| 1.8 | *Nhóm*: Phòng Tài Nguyên và Môi Trường | 1 | 36 | 0 | 36 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | HOANG-PC | 48E244A52997 | 192.168.1.127 | [LS] LS\_HUYEN VAN QUAN | UBND Xã Đồng Giáp | 71 |
| 2 | ADMIN-D79E8423C | D0DF9AA642E9 | 192.168.1.38 | [LS] LS\_HUYEN VAN QUAN | UBND Xã Trấn Ninh | 1 |
| 3 | LENOVO-PC | 5C93A2E18925 | 192.168.0.5 | [LS] LS\_HUYEN VAN QUAN | UBND Xã Đồng Giáp | 66 |
| 4 | DESKTOP-H7D7C64 | 907841D0CD9D | 192.168.1.42 | [LS] LS\_HUYEN VAN QUAN | UBND Xã Tú Xuyên | 13 |
| 5 | ADMIN | 446D57DEEE17 | 192.168.1.30 | [LS] LS\_HUYEN VAN QUAN | UBND Xã Trấn Ninh | 4 |
| 6 | WIN-T3013O2BFPM | B8EE655B9853 | 192.168.0.114 | [LS] LS\_HUYEN VAN QUAN | UBND Xã Khánh Khê | 1 |
| 7 | DESKTOP-AJVIHQ8 | B42E998D8D06 | 192.168.0.123 | [LS] LS\_HUYEN VAN QUAN | Trung tâm Văn hoá Thể thao và Truyền thông | 1 |
| 8 | LAPTOP-C6BIN5FS | 1063C8A6F3F9 | 192.168.0.110 | [LS] LS\_HUYEN VAN QUAN | Phòng Tài Nguyên và Môi Trường | 36 |
| 9 | ADMIN-PC | 58946BC85704 | 192.168.1.7 | [LS] LS\_HUYEN VAN QUAN | UBND Xã An Sơn | 54 |
| 10 | KHOPHANMEM24H | 40F02F9C8505 | 192.168.1.9 | [LS] LS\_HUYEN VAN QUAN | UBND Xã Hoà Bình | 18 |
| 11 | THU | 74C63B804EED | 192.168.1.2 | [LS] LS\_HUYEN VAN QUAN | UBND Xã An Sơn | 1 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [hacktool.win32.kmsauto.i!o](https://cloud.cmdd.vn/detail/virus/hacktool.win32.kmsauto.i!o) | 1 | 18 |
| 2 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 154 |
| 3 | [trojan.win32.exploinst.s!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.exploinst.s!o) | 5 | 1 |
| 4 | [virus.win32.agent.dp.d!o](https://cloud.cmdd.vn/detail/virus/virus.win32.agent.dp.d!o) | 3 | 1 |
| 5 | [trojan.win32.agent.ifdx!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.agent.ifdx!o) | 5 | 54 |
| 6 | [heur.win32.autoruninf.p](https://cloud.cmdd.vn/detail/virus/heur.win32.autoruninf.p) | 1 | 1 |
| 7 | [email-worm.win32.brontok!o](https://cloud.cmdd.vn/detail/virus/email-worm.win32.brontok!o) | 2 | 1 |
| 8 | [trojan.win32.hjclient.lnk.s!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.hjclient.lnk.s!o) | 5 | 36 |

1. HUYỆN TRÀNG ĐỊNH
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_HUYEN TRANG DINH | 6 | 61 | 54 | 7 |
| 1.1 | *Nhóm*: Xã Đào Viên | 3 | 55 | 53 | 2 |
| 1.2 | *Nhóm*: Xã Quốc Việt | 2 | 3 | 1 | 2 |
| 1.3 | *Nhóm*: Xã Tân Tiến | 1 | 3 | 0 | 3 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | HT-PC | 083E8EA54A05 | 192.168.1.7 | [LS] LS\_HUYEN TRANG DINH | Xã Tân Tiến | 3 |
| 2 | DESKTOP-SH0V0SG | E4F89CFE94FD | 192.168.1.22 | [LS] LS\_HUYEN TRANG DINH | Xã Đào Viên | 1 |
| 3 | 3PC | 00E1B0112070 | 192.168.1.3 | [LS] LS\_HUYEN TRANG DINH | Xã Quốc Việt | 1 |
| 4 | DESKTOP-UNTKQPO | EC5C68CDF6EF | 192.168.1.2 | [LS] LS\_HUYEN TRANG DINH | Xã Đào Viên | 47 |
| 5 | DIACHINH-PC | B8AEEDB7F425 | 192.168.1.9 | [LS] LS\_HUYEN TRANG DINH | Xã Quốc Việt | 2 |
| 6 | WIN-QOEVRO8SR5T | BC855647E88D | 192.168.0.3 | [LS] LS\_HUYEN TRANG DINH | Xã Đào Viên | 7 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.wminer4.s!m](https://cloud.cmdd.vn/detail/virus/trojan.win32.wminer4.s!m) | 5 | 2 |
| 2 | [virus.win32.virut.1!o](https://cloud.cmdd.vn/detail/virus/virus.win32.virut.1!o) | 3 | 2 |
| 3 | [trojan-ransom.win32!o](https://cloud.cmdd.vn/detail/virus/trojan-ransom.win32!o) | 5 | 1 |
| 4 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 11 |
| 5 | [trojan.win32.fakeapp!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.fakeapp!o) | 5 | 21 |
| 6 | [trojan.win32.agent!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.agent!o) | 5 | 1 |
| 7 | [trojan-spy.win32!o](https://cloud.cmdd.vn/detail/virus/trojan-spy.win32!o) | 5 | 19 |
| 8 | [trojan.win32.patched.qw!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.patched.qw!o) | 5 | 4 |

1. HUYỆN LỘC BÌNH
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_HUYEN LOC BINH | 7 | 20 | 10 | 10 |
| 1.1 | *Nhóm*: xã Thống Nhất | 2 | 12 | 6 | 6 |
| 1.2 | *Nhóm*: TT Lộc Bình | 3 | 4 | 2 | 2 |
| 1.3 | *Nhóm*: xã Hữu Khánh | 2 | 4 | 2 | 2 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | PC | 782BCBA05DB4 | 192.168.1.12 | [LS] LS\_HUYEN LOC BINH | TT Lộc Bình | 1 |
| 2 | PC | 00E04C3F3B46 | 10.116.174.130 | [LS] LS\_HUYEN LOC BINH | TT Lộc Bình | 1 |
| 3 | DHC-PC | 2CFDA174B6C3 | 192.168.2.147 | [LS] LS\_HUYEN LOC BINH | xã Thống Nhất | 6 |
| 4 | VPTULS010410 | 4CCC6A2E683E | 192.168.0.103 | [LS] LS\_HUYEN LOC BINH | TT Lộc Bình | 2 |
| 5 | ADMIN | 1C1B0DF6F131 | 192.168.1.15 | [LS] LS\_HUYEN LOC BINH | xã Hữu Khánh | 2 |
| 6 | THANHBINH-PC | D46A6A24CB01 | 192.168.2.114 | [LS] LS\_HUYEN LOC BINH | xã Thống Nhất | 6 |
| 7 | ADMIN | 309C235DFBFE | 192.168.0.113 | [LS] LS\_HUYEN LOC BINH | xã Hữu Khánh | 2 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.fakeusb!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.fakeusb!o) | 5 | 2 |
| 2 | [trojan-ransom.win32.blocker!o](https://cloud.cmdd.vn/detail/virus/trojan-ransom.win32.blocker!o) | 5 | 8 |
| 3 | [trojan.win32.wminer4.s!m](https://cloud.cmdd.vn/detail/virus/trojan.win32.wminer4.s!m) | 5 | 4 |
| 4 | [virus.win32.hvqb.s!o](https://cloud.cmdd.vn/detail/virus/virus.win32.hvqb.s!o) | 3 | 6 |

1. HUYỆN BẮC SƠN
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_HUYEN BAC SON | 3 | 61 | 26 | 35 |
| 1.1 | *Nhóm*: Phòng Nội Vụ | 1 | 28 | 26 | 2 |
| 1.2 | *Nhóm*: Thanh tra huyện | 1 | 31 | 0 | 31 |
| 1.3 | *Nhóm*: Các Phòng, ban chuyên môn | 1 | 2 | 0 | 2 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | NTH95-20200814H | 74D435626EC0 | 192.168.0.101 | [LS] LS\_HUYEN BAC SON | Thanh tra huyện | 31 |
| 2 | CHIEN-20200422G | 00251144EC21 | 192.168.1.27 | [LS] LS\_HUYEN BAC SON | Phòng Nội Vụ | 28 |
| 3 | ADMIN-TA | B8975AAF0CB0 | 192.168.1.42 | [LS] LS\_HUYEN BAC SON | Các Phòng, ban chuyên môn | 2 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.shadowbrokers!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shadowbrokers!o) | 5 | 4 |
| 2 | [exploit.win32.shadowbrokers!o](https://cloud.cmdd.vn/detail/virus/exploit.win32.shadowbrokers!o) | 5 | 1 |
| 3 | [trojan.win32.fakeapp!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.fakeapp!o) | 5 | 31 |
| 4 | [trojan.win32.wminer4.s!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.wminer4.s!o) | 5 | 3 |
| 5 | [hacktool.win32.shadowbrokers!o](https://cloud.cmdd.vn/detail/virus/hacktool.win32.shadowbrokers!o) | 1 | 1 |
| 6 | [trojan.win32.wminer4.s!m](https://cloud.cmdd.vn/detail/virus/trojan.win32.wminer4.s!m) | 5 | 4 |
| 7 | [trojan.win32.llac!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.llac!o) | 5 | 1 |
| 8 | [trojan.win32.generiz.s!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.generiz.s!o) | 5 | 16 |

1. BQL KHU KINH TẾ CỬA KHẨU ĐỒNG ĐĂNG
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_BQL KHU KT CUA KHAU DONG DANG | 2 | 23 | 12 | 11 |
| 1.1 | *Nhóm*: Phòng Quản lý Hạ tầng | 1 | 20 | 12 | 8 |
| 1.2 | *Nhóm*: Phòng Kế hoạch tổng hợp | 1 | 3 | 0 | 3 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | WY3YU9FSEPG1BF2 | F48E38B86F9A | 10.116.178.186 | [LS] LS\_BQL KHU KT CUA KHAU DONG DANG | Phòng Quản lý Hạ tầng | 20 |
| 2 | SON | 2CFDA1E26BF8 | 10.116.178.23 | [LS] LS\_BQL KHU KT CUA KHAU DONG DANG | Phòng Kế hoạch tổng hợp | 3 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan.win32.patched.qw!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.patched.qw!o) | 5 | 12 |
| 2 | [trojan.win32.gamaru.s!m](https://cloud.cmdd.vn/detail/virus/trojan.win32.gamaru.s!m) | 5 | 8 |
| 3 | [trojan.win32.shortcut.p!o](https://cloud.cmdd.vn/detail/virus/trojan.win32.shortcut.p!o) | 5 | 3 |

1. BAN DÂN TỘC
2. **Báo cáo tổng hợp virus mã độc trong hệ thống:** Trong quá trình rà quét và kiểm tra thực tế đã phát hiện được các máy tính bị lây nhiễm virus trong hệ thống

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Máy chủ** | **Máy trạm** | **Lây nhiễm** | **Đã diệt** | **Cách ly** |
| 1 | [LS] LS\_BAN DAN TOC | 1 | 4 | 0 | 4 |
| 1.1 | *Nhóm*: Văn phòng ban | 1 | 4 | 0 | 4 |

1. **Chi tiết các máy trạm bị lây nhiễm:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Máy tính** | **MAC** | **IP** | **Máy chủ** | **Nhóm** | **Số lần** |
| 1 | MANHLINH-PC | FCAA14B2991C | 192.168.2.106 | [LS] LS\_BAN DAN TOC | Văn phòng ban | 4 |

1. **Bảng mô tả chi tiết các loại virus lây nhiễm trên hệ thống:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên** | **Câp độ** | **Số lần** |
| 1 | [trojan-ransom.win32!o](https://cloud.cmdd.vn/detail/virus/trojan-ransom.win32!o) | 5 | 3 |
| 2 | [virus.win32.hvqb.s!o](https://cloud.cmdd.vn/detail/virus/virus.win32.hvqb.s!o) | 3 | 1 |

# **KẾT LUẬN ĐƯA RA KHUYẾN NGHỊ CHUNG:**

* + Đề xuất kiểm tra cập nhật các bản vá lỗi hệ điều hành thường xuyên.
  + Không tự ý cài các phần mềm không rõ nguồn gốc. Nên nhờ IT để kiểm tra trước khi cài vào máy.
  + Cài đặt và bật chức năng bảo vệ thời gian thực của phần mềm diệt virus CMC AV.
  + Định kỳ quét mã độc kiểm tra toàn bộ hệ thống máy tính, phòng tránh lây lan mã độc qua mạng.
  + Tắt hoặc kiểm tra lại chức năng Autorun của máy tính có kích hoạt phần mềm lạ nào không
  + Đặt mật khẩu mạnh cho tất cả các tài khoản, mở chức năng xác thực hai bước, đổi lại mật khẩu định kỳ.
  + Để có thể bảo vệ máy trạm không bị nhiễm lại những loại malware yêu cầu người dùng cập nhật bản vá bảo mật mới nhất của Windows được cung cấp.
  + Các bản cập nhật bảo mật cần thiết:
    - Windows 10 phiên bản 1909
    - Windows 8.1 và Windows Server 2012 R2 KB4499165 (Security-only update)
    - Windows 7 SP1 và Windows Server 2008 R2 SP1 KB4499175 (Security-only update)